Safeguarding Customer Information
An ABA Toolbox

The ABA is proud to offer this toolbox - free to ABA members - to assist bankers in safeguarding their customer information.

Financial institutions have had security programs in place for years, and have always recognized the trust that customers place in them to safeguard their financial information. With the passage of the Gramm-Leach-Bliley Act and the increased use of technology by both your institution and your customers, the security bar has been raised even higher. Your bank board also has specific responsibilities and concerns regarding information security that must be addressed.

Your institution's information security program thus must satisfy the concerns of three stakeholder groups, your customers and community, your board and shareholders, and your regulator.

The public portions of your program, as described in your security policy, your privacy notices and other communications should help your customers understand and feel comfortable with the steps you take as their financial institution to secure their information. Your security policy and program, as outlined and approved by your board, should give your board the level of comfort necessary to know the institution's security program is being managed properly and that they have fulfilled their fiduciary responsibilities. Your security program must also demonstrate to your regulator that you have assessed the risks to your customer's information and have controls in place to manage those risks.

Your Security Program Has Three Audiences
• **About The Toolbox**
  - Toolbox Users Guide
  - Guidelines at a Glance: Safeguarding Customer Information

• **Tool 1: Building Your Security Culture: From the Board Room to the Back Room**
  - Board and Senior Management Responsibilities
  - The Board Resolution
  - Codes of Conduct
  - Security and Other Officer Responsibilities
  - Technology Planning Questionnaire

• **Tool 2: Assessing Information Security and Risk in Your Institution**
  - The Risk Assessment Process
  - Assessing Your Customer Information Sharing Practices
  - Information Inventory and Risk Assessment
  - Intrusion Risk Assessment and Mitigation

• **Tool 3: Managing and Controlling Risk**
  - Writing Your Information Security Policy
    - Sample Policy 1
    - Sample Policy 2
    - Sample Policy 3
    - Sample Policy 4
  - Setting Employee Responsibility
  - Cybersecurity Checklist
  - Information Security Access Assessment
  - Remote Access Security Tips
  - Authentication Practices

• **Tool 4: Outsourcing Information Technology**
  - About Outsourcing
  - Twenty-Five Steps to Service Provider Selection
  - Service Provider Demonstration Questionnaire
  - Client Reference Questionnaire
  - Requests for Proposals
  - Service Level Agreements
  - Annual Reviews of Service Providers

• **Tool 5: Business Continuity and Disaster Recovery**
  - Structuring Your Business Continuity Plan
  - Disaster Recovery Planning – An Overview
  - Business Continuity Service Provider Survey

• **Tool 6: Training Your Employees**
  - Setting Your Security Training Requirements
  - Information Security in the Workplace
  - Information Technology Security Training Requirements
  - Privacy and Awareness Tips for Employees
  - Spotting and Avoiding Pretext Calls

• **Tool 7: Communicating Your Security Practices**
  - Security and Your Privacy Policy
  - Identity Theft and Resolution Self-Assessment
These tools build on the successful **ABA Financial Privacy Toolbox**, allowing you to incorporate, into your security program, the programs and procedures already in place to ensure that the privacy and security of customer information remain core values in all corners of your institution.

**About the Toolbox**

This ABA members-only toolbox, **Safeguarding Customer Information**, is a product of the ABA eStrategies Group, which is dedicated to providing you with resources and solutions to help you with your technology decisions.

While the ABA has developed a series of toolboxes over the years to assist members in a wide variety of areas, this particular tool is the first the association has developed that fully utilizes the power of the Web. You will find that each document contains a wide variety of links to worksheets, questionnaires, and other tools to assist you in your efforts to safeguard customer information.

The online nature of the toolbox also allows it to be a dynamic set of documents, allowing you as ABA members to continue to look to the tools for assistance in the future, even as the technology and security environment changes over time.

The toolbox has been designed around the recent **Examination Procedures** devised by the regulators to evaluate your compliance with the **Guidelines to Safeguard Customer Information**. We have used these procedures as the basic roadmap through much of the toolbox. At the same time, the tools are designed to take you beyond Gramm-Leach-Bliley, helping you not only comply with GLB but also with determining whether your technology and business strategies are properly aligned.

The toolbox could not have been completed without the assistance of a number of individuals and organizations, a list that will continue to grow as we build on and improve these tools. Ken Proctor of Alex Sheshunoff Management Services, Inc., and Stephen Ryan from the BISYS Group assisted with the technology planning questionnaire, technology inventory, as well as the client reference and demonstration questionnaires. Wayne Barnett and Mary Beth Guard through BankersOnline contributed several of the sample security policies and the information security access assessment. Red Siren Technologies developed the cybersecurity checklist. Roseanne Rostron of RISConsulting LLC contributed the service provider business continuity questionnaire. The sections on authentication practices and "About Outsourcing" are adapted from the work of Brad Beytien from the Federal Reserve Bank of Kansas City. The Federal Deposit Insurance Corporation contributed the request for proposal and service level agreement tools. Security Education Systems contributed to the disaster recovery tools. And Rob Douglas of American Privacy Consultants, Inc, provided pretext calling training guides. We are grateful to all of our contributors.

**Toolbox Users Guide**

Protecting our customers’ personal financial information has always been part and parcel of banking, and it remains the cornerstone of our industry today. But the information age is changing how we collect and store customer data, making it very important to re-examine how we protect customer information. Simply put, the security systems that worked well in the past may need to be retooled for today’s world.

In August 2000, the American Bankers Association completed the development of a **Financial Privacy Toolbox** under the tutelage of the ABA Task Force on Responsible Use and Protection of Customer Information. The Task Force members were drawn from institutions of all sizes and from all parts of the country. It also included representatives of non-bank affiliates and third-party providers.

As the name of our task force implies, the responsible use and the protection of customer information go hand-in-hand. Thus the voluntary guidelines for the responsible use and protection of customer information
that the task force developed are as relevant for the purposes of safeguarding customer information as they are for its responsible use.

What the Toolbox Does

The ABA Safeguarding Customer Information Toolbox thus supplements our Financial Privacy Toolbox, providing tools to help your institution establish a comprehensive customer information security program. Each section is designed to be flexible, providing options where possible to suit a variety of organizational styles, sizes and information management practices.

The worksheets, questionnaires and other tools can be used separately or together to ensure that your institution has a program that not only complies with Section 501(b) of the Gramm-Leach-Bliley Act, but also ensures that your policy is consistently understood and enforced throughout your institution.

Whatever the size or complexity of your institution, the toolbox is designed to help you:

- Build a culture where every employee and board member understands the importance of safeguarding customer information and understands his or her role in the process.
- Assess the risks to your customer information and other databases and systems and manage those risks.
- Assess and manage your third party technology service providers and incorporate this review into your risk assessment and security program.
- Set your business continuity planning and disaster recovery objectives and policy.
- Ensure that your employees have the security training and experience appropriate for their position.
- Communicate your security program to your customers in a way that they can understand and be comfortable with your efforts to secure their financial and other information.

How The Toolbox Is Organized

The toolbox is divided into seven separate tools.

1. **Building Your Security Culture: From the Board Room to the Back Room.** The objective of this tool is to help you put in place the organization to govern and manage your information security program. The tool outlines the responsibilities of the board and others under the GLB Act, as well as providing a sample board resolution and several examples of codes of conduct that your institution can use to alert employees of their security obligations.

2. **Assessing Information Security and Risk in Your Institution.** This tool provides you a basis for assessing your current technology environment, how your customer information is housed within that environment, and then most importantly gives you a framework for assessing and quantifying the risks to you customer information from disclosure, fraud or errors, or unavailability.

3. **Managing and Controlling Risk: Gramm-Leach-Bliley and Beyond.** This tool assists you in putting the controls and policies in place to protect customer information and applications, consistent with the risk presented to those applications.

4. **Outsourcing Information Technology.** This tool is designed to help you assess outsourcing risk, incorporate that risk assessment into the selection process, and then manage the outsourcing relationship contingent upon the risk it presents to your institution.
5. **Business Continuity and Disaster Recovery.** This tool provides you with a framework to protect your institution against destruction, loss, or damage of customer information from potential hazards, and to recover if in fact they occur.

6. **Training Your Employees.** This tool assists you in determining any gaps in the security training and experience of your employees, depending upon their functions within your institution.

7. **Talking About Security: Communicating with Customers.** This final tool provides potential language for you to use within your privacy and security policy and notices so that your customers know of your commitment to them. Lastly, this tool contains the recently completed **ABA Crisis Communications Kit**, developed by ABA’s Public Relations Department to assist you discussing a disaster or other crisis with your stakeholder and it’s impact on your institution.

A useful “**Guidelines at a Glance: Safeguarding Customer Information,**” is included and is used as a roadmap throughout this toolbox as a reference guide to the key questions and considerations confronting your institution as you refine our security program.

### Guidelines at a Glance

Section 501(b) of GLBA requires federal banking agencies to establish appropriate standards for the administrative, technical, and physical safeguards for customers’ “nonpublic personal information.” To accomplish this congressional mandate, each agency has issued guidelines that require each bank to establish an information security program. These guidelines are separate and apart from the privacy regulations and notice requirements contained in Section 501 of GLBA.

A bank’s information security program must be designed to ensure the security and confidentiality of customer information, protect against any anticipated threats or hazards to the security or integrity of such information, and protect against unauthorized access to or use of such information that would result in substantial harm or inconvenience to any customer.

Because the guidelines closely mirror existing agency guidance, in many instances financial institutions will already have information security programs that identify and control risks to information and information systems. While the guidelines cover only “customer information” as that term is defined, the agencies encourage institutions to use the approach provided by the guidelines to protect all customer and bank records.

The agencies have promulgated a set of uniform examination procedures that we have incorporated intended to assist examiners in assessing the level of compliance with the security guidelines that we have incorporated in ‘**Guidelines at a Glance: Safeguarding Customer Information.**’ We have used these guidelines as a roadmap throughout this toolbox as a reference guide to the key questions and considerations confronting your institution as you refine your security program. The guidelines allow each institution the discretion to design an information security program that suits its particular size and complexity and the nature and scope of its activities. At the same time, each institution must demonstrate that its security program addresses the following:

**Role of the Board of Directors.** The board of directors or an appropriate committee of the board is responsible for approving the written information security program and overseeing the program’s development, implementation, and maintenance, including assigning responsibility for its implementation. At least once a year, management should provide a status report to the board or the appropriate committee.

**Identify and Assess Risk.** The institution should first assess risks to its customer information. An institution’s risk assessment should identify reasonably foreseeable internal and external threats that could result in unauthorized disclosure, misuse, alteration, or destruction of customer information or customer information systems. Additionally, the risk assessment should consider the likelihood and potential damage of these threats, taking into consideration the sensitivity of customer information. Finally, the assessment should consider the sufficiency of existing policies, procedures, customer information systems, and other arrangements intended to control the risks identified.
**Manage and Control of Risk.** The institution should design an information security program to control the identified risks, commensurate with the sensitivity of the information and the complexity and scope of the bank’s activities. The guidelines highlight **eight security measures** that institutions should consider and adopt if appropriate.

The information security program also should include training for staff and regular testing of the key controls, systems, and procedures. The nature and frequency of the tests should be determined by the institution’s risk assessment. To ensure objectivity, tests should be conducted or reviewed by third parties or staff who are independent of those who develop or maintain the security programs.

**Oversee Service Provider Arrangements.** Institutions also have an obligation to oversee their service providers. Institutions that use service providers should exercise appropriate due diligence in selecting them, including conducting a review of the measures taken by the service providers to protect customer information. The contract between the institution and the service provider must require the provider to implement appropriate measures designed to meet the objectives of the guidelines. Wherever indicated by an institution’s risk assessment, the institution should monitor its service providers to confirm they are implementing the agreed-upon security measures. As part of this monitoring, an institution should review audits, summaries of test results, or other equivalent evaluations of its service providers.

**Adjust the Program.** Risks to customer information change over time with changes in technology, the sensitivity of customer information, internal or external threats to information, and the institution’s own business arrangements, such as mergers and acquisitions, alliances and joint ventures, outsourcing arrangements, and changes to customer information systems. Therefore, institutions should monitor, evaluate, and adjust, as appropriate, their information security program. The regulatory agencies expects institutions to make the appropriate changes to their information security programs before any changes are made to their customer information systems.

**Implement the Guidelines.** The guidelines were effective on July 1, 2001. However, there is a two-year grandfathering provision for service provider contracts. Existing service provider contracts (namely, contracts entered into until March 5, 2001) do not have to be renegotiated to comply with the guidelines until July 1, 2003.

The regulatory agencies have adopted uniform examination procedures intended to assist examiners in assessing the level of compliance with the guidelines. These procedures are designed to apply to a wide range of banks, and as such examiners have been instructed that certain procedures may not apply to smaller or less complex institutions. Institutions should be prepared to detail for examiners the reasons why a particular procedure is not applicable, based on the institutions size, complexity, or risk assessment.

<table>
<thead>
<tr>
<th>Guidelines At A Glance: Safeguarding Customer Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Key Questions or Considerations</strong></td>
</tr>
<tr>
<td>I. Determining The Involvement Of The Board.</td>
</tr>
<tr>
<td>A. Has the board or its designated committee approved a written Corporate Information Security Program that meets the requirements of the Information Security Guidelines (guidelines)?</td>
</tr>
<tr>
<td>B. If the board has assigned responsibility for program implementation and review of management reports to an individual or committee, do they possess the necessary knowledge, expertise and authority to perform the task?</td>
</tr>
<tr>
<td>C. Does the program contain the required elements?</td>
</tr>
<tr>
<td>1. If more than one information security program exists for the institution, are the programs coordinated across organizational units?</td>
</tr>
<tr>
<td>D. Determine the usefulness of reports from management to the board (or its designated committee). Does the report adequately describe the overall status of the program, material risk issues, risk assessment, risk management and control decisions, service provider oversight, results of testing, security breaches and management's response, and recommendations for program changes?</td>
</tr>
</tbody>
</table>
1. How often does the board (or its designated committee) review reports?

E. Overall, do management and the board (or its designated committee) adequately oversee the institution's information security program?

## II. Evaluating The Risk Assessment Process.

### A. Review the risk assessment program.

1. How does the institution assess risk to its customer information systems and non-public customer information?

2. Has the institution evaluated the risk to the entire customer information system?

3. Has the institution used personnel with sufficient expertise to assess the risks to its systems and customer information on an enterprise-wide basis?

4. Is the risk assessment part of a formal risk assessment process with timelines and milestones? If not, how will management ensure timely completion?

5. Does the institution have a process for identifying and ranking its information assets (data and system components) according to sensitivity? How does it use this process in its risk assessment?

### B. Assess adequacy and effectiveness of risk assessment process.

1. Does the institution identify all reasonably foreseeable internal and external threats that could result in unauthorized disclosure, misuse, alteration, or destruction of customer information or customer information systems?

2. Does the institution support its estimate of the potential damage posed by various threats?

3. Review the institution’s existing controls to mitigate risks. Does the institution’s analysis consider the current administrative, physical, and technical safeguards that prevent or mitigate potential damage?

4. Does the institution use test results to support its assessment of the adequacy and effectiveness of those controls?

### C. Does the institution identify and prioritize its risk exposure, decide on the risks it must mitigate, and create a mitigation strategy? Is the decision to accept risks documented and reported to the appropriate management levels?

1. Does the institution promptly act to mitigate risks that pose the immediate possibility of material loss?

2. How does the institution demonstrate that the mitigation strategy was reviewed by appropriate officials?

3. Does the risk assessment provide guidance for the nature and extent of testing?

4. Does the risk assessment include vendor oversight requirements?

## III. Evaluating The Adequacy Of The Program To Manage And Control Risk.

### A. Review internal controls and policies. Has the institution documented or otherwise demonstrated, at a minimum, that it considered the following controls, and adopted those it considered appropriate?

1. Access controls, such as controls to authenticate and permit access to customer information systems to authorized persons only.

2. Access restrictions at physical locations, such as buildings and computer facilities, to permit access to authorized persons only.

3. Encryption of electronically transmitted and stored customer data.

4. Procedures to ensure that systems modifications are consistent with the approved security program.
<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>5.</td>
<td>Dual control procedures, segregation of duties, and employee background checks.</td>
<td></td>
</tr>
<tr>
<td>6.</td>
<td>Monitoring systems and procedures to detect actual and attempted attacks on or intrusions into customer information systems.</td>
<td></td>
</tr>
<tr>
<td>7.</td>
<td>Response programs specifying actions to be taken by specific individuals when the institution suspects unauthorized access (i.e., incident response).</td>
<td></td>
</tr>
<tr>
<td>8.</td>
<td>Measures to protect against destruction, loss, or damage of information from potential environmental hazards, such as fire and water damage or technological failures.</td>
<td></td>
</tr>
<tr>
<td>B.</td>
<td>Is staff adequately trained to implement the security program?</td>
<td></td>
</tr>
<tr>
<td>1.</td>
<td>Obtain from management a listing of the training provided to all users of the institution’s system.</td>
<td></td>
</tr>
<tr>
<td>C.</td>
<td>Determine whether key controls, systems, and procedures of the information security program are regularly tested by independent third parties or qualified independent staff in accordance with the risk assessment.</td>
<td></td>
</tr>
<tr>
<td>1.</td>
<td>Assess whether the nature and frequency of testing is consistent with the risk assessment.</td>
<td></td>
</tr>
<tr>
<td>2.</td>
<td>Assess whether tests are conducted or reviewed by independent third parties or qualified staff independent of those that develop or maintain the security program.</td>
<td></td>
</tr>
<tr>
<td>3.</td>
<td>Assess whether management reviews test results promptly. Assess whether management takes appropriate steps to address adverse test results.</td>
<td></td>
</tr>
<tr>
<td>IV. Assessing The Measures Taken To Oversee Service Providers.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>A.</td>
<td>Determine whether the institution exercises due diligence in selecting service providers.</td>
<td></td>
</tr>
<tr>
<td>B.</td>
<td>Determine what information is supplied to service providers.</td>
<td></td>
</tr>
<tr>
<td>C.</td>
<td>Obtain a copy of the contract(s) with the service provider(s). Determine whether contracts require service providers to implement appropriate measures to meet the objectives of the guidelines.</td>
<td></td>
</tr>
<tr>
<td>D.</td>
<td>If the institution’s risk assessment requires monitoring a service provider, then perform the following steps for each applicable service provider.</td>
<td></td>
</tr>
<tr>
<td>1.</td>
<td>Determine whether the service provider contract provides for sufficient reporting from the service provider to allow the institution to appropriately evaluate the service provider’s performance and security, both in ongoing operations and when malicious activity is suspected or known.</td>
<td></td>
</tr>
<tr>
<td>2.</td>
<td>Determine whether the institution’s actions adequately control information supplied to service providers, ensuring that the information is managed and secured properly.</td>
<td></td>
</tr>
<tr>
<td>3.</td>
<td>Review financial condition of service provider.</td>
<td></td>
</tr>
<tr>
<td>V. Determining Whether An Effective Process Exists To Adjust Program.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>A.</td>
<td>Does the institution have an effective process to adjust the information security program as needed? Is the appropriate person assigned responsibility for adjusting the information security program?</td>
<td></td>
</tr>
<tr>
<td>B.</td>
<td>Review procedures that are in place to ensure that when the institution makes changes in technology and its business function the requirements of the guidelines are also considered. These changes can include:</td>
<td></td>
</tr>
<tr>
<td>1)</td>
<td>Technology changes (e.g., software patches, new attack technologies and methodologies).</td>
<td></td>
</tr>
<tr>
<td>2)</td>
<td>Sensitivity of information.</td>
<td></td>
</tr>
<tr>
<td>3)</td>
<td>Threats (both nature and extent).</td>
<td></td>
</tr>
<tr>
<td>4)</td>
<td>Upcoming changes to institution’s business arrangements (e.g., mergers and acquisitions, alliances and joint ventures, outsourcing arrangements).</td>
<td></td>
</tr>
</tbody>
</table>
| 5) | Upcoming changes to customer information systems (e.g., new configurations or connectivity, new.
C. Determine whether appropriate expertise is applied to evaluate whether changes to the information security program are necessary.

D. Determine whether appropriate controls exist to ensure changes to the information security program are properly implemented in a timely, risk-based manner.

Tool 1: Building Your Security Culture
From The Board Room To The Back Room

Building a culture where every employee understands the importance of safeguarding customer information is a vital step toward fulfilling your obligations under Gramm-Leach-Bliley and setting the proper tone for your institution.

A financial institution’s overall information security program is critical to the safety and soundness of the institution. It is for this reason that the agencies placed the responsibility on an institution’s board to approve and exercise general oversight over the program. This tool outlines the responsibilities of the board and others under the GLB Act, and provides a sample board resolution and several examples of codes of conduct that your institution can use to alert employees of their security obligations.

Lastly, this tool can assist you in defining the lines of authority and responsibility for development, implementation, and administration of your financial institution’s information security program.

Board and Senior Management Responsibilities

A financial institution’s overall information security program is critical to the safety and soundness of the institution. It is for this reason that the agencies placed the responsibility on an institution’s board to approve and exercise general oversight over the program. The Gramm-Leach-Bliley 501(b) examination procedures contain the following Key Questions or Considerations regarding board and senior management involvement in the security program process. The column outlining “What Your Institution Should Consider” is derived from the regulatory clarifications, supplemented with other suggested actions for the institution to consider.
<table>
<thead>
<tr>
<th>Key Questions or Considerations</th>
<th>What Your Institution Should Consider</th>
</tr>
</thead>
</table>
| A. Has the board or its designated committee approved a written Corporate Information Security Program that meets the requirements of the Information Security Guidelines? | 1. Conduct and document a risk assessment outlining your security program and its appropriateness for the size and complexity of your institution and the nature and scope of its activities.  
2. Document that the board or its designated committee has approved the program. Board or committee minutes should reflect involvement in overseeing and coordinating information technology resources. |
| B. If the board has assigned responsibility for program implementation and review of management reports to an individual or committee, do they possess the necessary knowledge, expertise and authority to perform the task? | If your board delegates this authority, document that the qualifications of the individual or committee have been reviewed. Examiners will review organizational charts, job descriptions, compensation, turnover, and training programs to ensure that the institution has a sufficient number of technology personnel and that these personnel have the appropriate expertise. |
| C. Does the program contain the required elements? | The GLB Act requires the following eight elements to be part of the institution's security program:  
1. Access controls, such as controls to authenticate and permit access to customer information systems to authorized persons only.  
2. Access restrictions at physical locations, such as buildings and computer facilities, to permit access to authorized persons only.  
3. Encryption of electronically transmitted and stored customer data.  
4. Procedures to ensure that systems modifications are consistent with the approved security program.  
5. Dual control procedures, segregation of duties, and employee background checks.  
6. Monitoring systems and procedures to detect actual and attempted attacks on or intrusions into customer information systems.  
7. Response programs specifying actions to be taken by specific individuals when the institution suspects unauthorized access (i.e., incident response).  
8. Measures to protect against destruction, loss, or damage of information from potential... |
### Guidelines at a Glance: Determining the Involvement of the Board

<table>
<thead>
<tr>
<th>Key Questions or Considerations</th>
<th>What Your Institution Should Consider</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>environmental hazards, such as fire and water damage or technological failures.</td>
</tr>
<tr>
<td>1. If more than one information security program exists for the institution, are the programs coordinated across organizational units?</td>
<td>Determine whether an enterprise-wide coordination of information security programs exists. Coordination should encompass all elements of the information security programs. One master program is not required.</td>
</tr>
<tr>
<td>D. Determine the usefulness of reports from management to the board (or its designated committee).</td>
<td>Reports should adequately describe the overall status of the program, material risk issues, risk assessment, risk management and control decisions, service provider oversight, results of testing, security breaches and management's response, and recommendations for program changes.</td>
</tr>
<tr>
<td>1. How often does the board (or its designated committee) review reports?</td>
<td>Reports on compliance with guidelines should be presented to the board (or its designated committee) at least annually.</td>
</tr>
<tr>
<td>E. Overall, do management and the board (or its designated committee) adequately oversee the institution's information security program?</td>
<td>Board or committee minutes should demonstrate the level of involvement in the oversight process by the board (or its designated committee) and involvement by senior management. Examiners will want to review documentation supporting major projects or initiatives to determine the effectiveness of technology planning, implementation, and follow-up activities. Examiners may consider:</td>
</tr>
<tr>
<td>1. The decision process, including options considered and the basis for the final selection.</td>
<td></td>
</tr>
<tr>
<td>2. The reasonableness of implementation plans.</td>
<td></td>
</tr>
<tr>
<td>3. The effectiveness of monitoring of implementation activities.</td>
<td></td>
</tr>
<tr>
<td>4. Whether validation testing of new programs or systems is conducted prior to putting the programs into production.</td>
<td></td>
</tr>
</tbody>
</table>

### Board of Director Responsibilities

The guidelines allow the entire board of a financial institution, or an appropriate committee of the board, to approve the institution’s written security program. In addition, the guidelines permit the board to assign specific implementation responsibilities to a committee or an individual.

Thus an important decision for your full board to make is whether they chose to delegate this authority to the audit or other committee. For board of directors to make this decision, it needs to fully understand the
importance of protecting the security of information to your customers, your institution and our industry. There may be no more important group to educate than your board members. The training materials in Tool 5 can help begin this process.

**Consider a Board Resolution**

You can begin this process by having your board set the standards of responsible use and protection of customer information for your institution and every employee. A board resolution incorporating the voluntary guidelines of the ABA Task Force is one means to do this.

**Senior Management Responsibilities**

The day-to-day monitoring of all aspects of an information security program is a management responsibility. Each institution is in the best position to determine who should be assigned specific roles in implementing the institution’s security program. While the agencies have therefore not assigned specific roles, there are three general responsibilities of the institution in the development of an information security program:

1. Evaluate the impact on a financial institution’s security program of changing business arrangements and changes in customer information systems;

2. Document compliance with the guidelines; and

3. Keep the board informed of the overall status of the institution’s information security program.

Each financial institution must monitor, evaluate, and adjust its information security program in light of relevant changes in technology, the sensitivity of its customer information, internal or external threats to information, and the institutions’ own changing business arrangements. This would include an analysis of risks to customer information posed by new technology (and any needed program adjustment) before an institution adopts the technology in order to determine whether a security program remains adequate in light of the new risks that may be presented.

The agencies expect that in all cases, management will provide its board (or the appropriate board committee) a written report on the information security program consistent with the guidelines at least annually. Management of institutions with more complex information systems may find it necessary to provide information to the board (or a committee) on a more frequent basis. Similarly, more frequent reporting will be appropriate whenever a material event affecting the system occurs or a material modification is made.

**Building the Team**

Since customer information flows through all departments of your institution, senior management from those departments should be involved in the development and implementation of your information management/security program. The creation and implementation, and revision of the program require a team of individuals. Individuals from the business units of the institution, as well as those responsible for customer privacy, must have an active role in setting, articulating, and adhering to the information security standards set by the institution.

**Conducting an Information Self-Assessment**

An important step in the protection of customer information is the determination of “who owns the data,” that is, where is customer information housed and how is that information shared within and outside of your institution. Senior department management should conduct an Information Self-Assessment, contained in Tool 2, to answer questions such as “How do we collect customer information?” “How do we share customer information across the organization and with third parties?” “What are our current information security policies and procedures?”
The Board Resolution

If your institution did not consider a board resolution as part of the process of implementing the Gramm-Leach-Bliley Act’s privacy provisions, you may want to do so as part of your 501(b) compliance process. Such a resolution demonstrates to staff and to customers the commitment the board has toward the safe and responsible use of customer information and sets the right tone for the institution overall.

This board of director's resolution incorporates the voluntary industry guidelines contained within the ABA Financial Privacy Toolbox. You may wish to amend it as appropriate to address your institution’s specific practices.

The resolution should also be consistent with the statements you make within your privacy notices and security policy regarding the security of customer information. You may also wish to incorporate portions of any board resolution your institution adopts into a culture statement for your overall institution. Such an approach allows you to ensure that all three audiences you have for your security program receive a consistent message.

With corporate leadership and fiscal integrity in the national spotlight, the ABA has developed a members-only [link to Web clearinghouse] as a resource for you on corporate governance issues. Through the use of the tools on this page, financial institutions can reaffirm their long-standing commitment to the principles of corporate accountability. Check there often for updates.

Privacy and Security Pledge

Whereas [Institution Name] recognizes its customers’ expectations of financial privacy and security; and whereas preserving our customers’ trust and safeguarding our customer’s information are core values to our institution and the broader banking community; we therefore resolve to abide by the following guidelines for the responsible use and protection of our customers’ information:

✓ We will always value the trust of our customers and the importance of keeping their personal financial information confidential and secure.
✓ We will provide our customers with our policy on using their personal financial information responsibly and protecting it.
✓ We will hold our employees to the highest standard of conduct in ensuring the confidentiality and security of customer information.
✓ We will hold any personal medical information about our customers sacred and will NOT use it for marketing purposes or in making credit decisions.
✓ We will use information responsibly in order to provide our customers with significant benefits, including fraud prevention, improved products and services and to comply with laws.
✓ We will establish procedures to maintain accurate information and respond in a timely manner to our customers’ request to change or correct information.
✓ We will use a combination of safeguards to protect our customers against the criminal use of their information and to prevent unauthorized access to it.
✓ We will offer our customers the option of restricting information shared with third parties for marketing purposes and honor their preferences.
✓ We will require the companies we do business with to abide by our privacy and security policies to
Codes of Conduct

These sample codes of conduct are designed to help create an environment within your institution where all employees are aware of their responsibility to protect customer information.

SAMPLE 1:

Confidential Information and Personal Liability

Employees, directors and their associates may be held personally liable for using confidential information (obtained while serving as a director or employee) for personal benefit. They may also be subject to governmental or corporate administrative action. [Institution Name]’s business and customer information and any related files are confidential and cannot be disclosed to unauthorized persons (including competitors) without permission.

SAMPLE 2:

Confidentiality and Integrity of Information

Information about the Corporation, its affiliates, customers, suppliers and employees obtained by virtue of employment with the Corporation is confidential and must be treated as such. Information should neither be modified nor destroyed without proper approval. Disclosure of confidential information to unauthorized persons outside the company is prohibited.

Authentication

In keeping with our tradition of confidentiality, methods of customer authentication, such as an authorization code, are used whenever necessary in the ordinary course of business to obtain information of a confidential nature.

Accountability

It is the policy of [Institution Name] to treat all information regarding its customers and employees in strictest confidence. Failure to maintain the confidentiality of this information will result in corrective action, up to and including immediate dismissal.

SAMPLE 3:

Introduction

In implementing [Institution Name]’s vision in accordance with our values, this Code of Conduct (the Code) serves as a guide to ethical conduct for all employees of [Institution Name]. This policy covers areas of business conduct when working with clients, customers, suppliers, the public and other employees. It also addresses conflicts of interest, which could arise between the personal conduct of employees and their positions with [Institution Name].

Penalty for Violations

Employees are expected to act fairly and honestly when conducting business on behalf of [Institution Name], maintain [Institution Name]’s high ethical standards, and obey all applicable laws. Violations of the Code and applicable laws or failure to cooperate with an internal investigation may constitute grounds for corrective action, up to and including immediate dismissal.
Safeguarding Confidential Information

When conducting business, many employees may become privy to confidential information about [Institution Name], its present and prospective customers and suppliers, its stockholders and employees. Employees who possess such confidential information must understand that it has been given to them for an express business purpose, may be disclosed only on a need-to-know basis, and used only for a proper business purpose. Discretion should be used when confidential information is disclosed, and it should never be disseminated to unauthorized persons.

Misuse of confidential information may result in civil or criminal liability, or in sanctions or penalties against both [Institution Name] and the individual responsible for misusing such information.

Procedures to Restrict Flow of Information

Because [Institution Name] is a multi-service financial institution, banking and securities laws, as well as good business practices, require that [Institution Name] have procedures ("firewalls") to prevent material nonpublic information obtained while engaging in one of [Institution Name]'s diverse business activities from being utilized improperly by others within or outside of [Institution Name].

Security and Other Officer Responsibilities

While there is no requirement within the GLB Act to create a new position with a specific title of “Corporate Information Security Officer,” Regulation H, which implements the Bank Protection Act, states that your institution's board of directors is responsible for designating a Security Officer, who has the authority to research, develop and implement the institution's Security Program.

A financial institution will not need to create a new position, as long as the institution has adequate staff in light of the risks to its customer information. Regardless of whether new staff is added, the lines of authority and responsibility for development, implementation, and administration of a financial institution’s information security program need to be well defined and clearly articulated.

Emerging industry-standard professional qualifications for an institution's Security Officer include:

✓ Holding at least a mid-to-upper-level manager's or executive's position;
✓ Membership on the institution's Executive Committee;
✓ The ability to report directly to the board of directors or an independent audit committee about security matters;
✓ Experience in several operational areas;
✓ Education in both business management and the administration of justice;
✓ Not also being the auditor (your auditor should act as your investigative companion and as the person who documents investigations); and
✓ The fulfillment of other duties, so long as those duties does not compromise internal controls.

In that no two institutions are alike, the organizational structure and lines of responsibility and accountability for secure measures will naturally vary from institution to institution. In determining which structure works best for your institution, there are several things you may wish to consider:

1. How should day-to-day security responsibilities and the responsibilities for complying with the reporting requirements be segregated? The skills necessary for one are not necessarily the same as for the other.
2. To what extent can your internal teams of employees independently operate and test your customer information systems? Is your institution’s internal audit department sufficiently trained and independent for the purposes of testing key controls and providing test results to decision makers independent of system managers?

3. Have your human resources personnel developed a program designed to instill a culture of information security in your institution and train employees in their role in implementing the institution’s security program?

4. Does your institution have appropriate dual control procedures and segregation of duties for high-risk activities?

5. Are employee background checks conducted for employees with responsibility for, or access to, customer information?

How Many Hats Does Your Security Officer Wear?

Because in the past the security officer’s position was felt not to require full-time staffing, the person in charge of security at many institutions is used to being pulled into a variety of directions, being placed in charge of compliance as well as physical and cyber security. **When determining the duties of your head of security, it is important to maintain the separation between the audit and operational functions. Bottom line: if an individual with regulatory accountability has to “audit” himself or herself, the two functions should not be on the same employee.

The following security officer position description may be of some assistance to you, regardless of whether your institution determines to combine these duties into one position or have several individuals responsible for various aspects of security and compliance. The very breath of the responsibilities outlined for the security officer point to the need to build a team of individuals with the shared responsibility for the cyber as well as physical security of customer and other information.

Security Officer Position Description Sample

Purpose:

- Directing all internal and external security and loss prevention resources to reduce or eliminate losses from all sources.

Key Responsibilities:

- Developing, implementing and administering all segments of the institution’s Security Program, including physical, technical, personnel, procedural and electronic security.
- Providing continual consultation and written reports to senior management and to the board of directors concerning security issues.
- Working with the institution’s legal representative and department leaders, insuring that the institution’s employees, customers, facilities, assets, records and proprietary information are protected.
- Working with the institution’s human resources representative and department leaders, conducting and managing initial and continuing reviews of employment practices, confidentiality agreements, background investigations and drug screening practices, and approving security clearances.
- Working with other department leaders, designing security components for operations and other strategic processes, and supervising the development and implementation of required security reporting devices and processes at all levels.
- Selecting, maintaining and testing appropriate intrusion devices, alarms and cameras that record activity in appropriate locations and that warn of threats.
- Developing and implementing physical security procedures and processes for all of the institution's locations, plans for reducing or eliminating premises liability issues and site analysis and threat assessment documentation.
• Designing and implementing courier and armored car carrier processes.
• Developing and maintaining corporate investigative practices and standards, and investigating all suspected internal and external criminal violations, suspicious incidents and policy violations that may become security issues.
• Creating and retaining case management records for all investigations and Security Program operations.
• Managing coordinated legal process effort and loss recovery efforts.
• Developing, administering and delivering security training programs, involving front office and visitor security, security guard force and specialized training programs for executives, managers, special employees and field employees.
• Managing a Situation Management Team that addresses potential or in-progress violent events and other special projects.
• Working with other department leaders, assisting with the continual development of loss control and anti-compromise measures to protect general assets, proprietary information and processes.
• Conducting continual surveys of all offices, departments and functions to determine the need for additional security services, and making appropriate recommendations.
• Establishing and maintaining satisfactory liaison with law enforcement officers at all levels in geographical areas where employees and customers are located, and maintaining files for each location regarding available resources and emergency services agencies available.
• Supervising and directing personnel from other departments when conducting investigations.
• Supervising a guard force at appropriate locations.
• Preparing and submitting a Security Program evaluation and compliance report to the Board of Directors at least annually.

**Key Knowledge, Skills & Abilities**

• Highly-developed and proven leadership, management, investigation and negotiation skills.
• Highly developed and proven ability to initiate and manage projects that will affect other departments and functions, as well as the corporate environment.
• Highly-developed and proven oral and written communication skills.
• Significant knowledge of the security contracting process for personnel and equipment.
• Basic knowledge of financial investigation process models and applications, and flowcharting techniques.
• Basic knowledge of accounting, auditing, compliance processes and their interaction with the security function.
• Basic knowledge of guard service processes.

Intermediate knowledge of personal computer operation and use of basic business computer tools.
Instructions For Questionnaire

The Technology Planning Questionnaire is a self-scored assessment of your institution’s technology planning and administration process. The questionnaire and its scorecard can help identify your institution’s current technology environment, allowing you to “take your technology temperature” as a part of your information security process. It also helps your institution begin to identify the gap between your current capabilities, resources, requirements, infrastructure, and those that are needed in the future.

The questionnaire is divided into five sections:

- **Assessing the Planning Process**
- **Fostering Technology Human Resources**
- **Communicating Technology Strategy**
- **Judging Technology Effectiveness**
- **Matching Technology and Business Requirements**

Share this questionnaire and its results with executive management, department heads, and/or business line managers to gather their perspectives on current technology objectives, your existing technology environment, whether technology is being used and deployed effectively, as well as how well your institution communicates its technological direction.
Assessing the Planning Process

This worksheet will help your institution define the planning process and how it relates to your annual, strategic and technology initiatives. It also assesses how effective your institution’s plans are in supporting the goals of the institution. Circle the number that best describes your institution. Circling "STRONGLY AGREE" implies that the entire statement is true for the entire institution. Circling "STRONGLY DISAGREE" means that no part of the sentence is true.

<table>
<thead>
<tr>
<th></th>
<th>STRONGLY DISAGREE</th>
<th>DISAGREE</th>
<th>NEUTRAL</th>
<th>AGREE</th>
<th>STRONGLY AGREE</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. My institution has an accepted and well-documented annual business plan.</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>2. My institution has an accepted and well-documented long-term strategic plan.</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>3. My institution has an accepted and well-documented technology plan that includes security.</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>4. My technology plan is closely aligned with both my annual and long-term strategic plans.</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>5. My technology plan addresses each line of business and distribution channel.</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>6. My technology plan considers future products and services not currently offered by my institution.</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>7. My institution has the capability and means to assess the effectiveness of our technology plan across all products and channels.</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>8. My institution has the tools to measure the economic and business impact of our technology plan on the overall success of our institution.</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>9. My institution's lines of business and technology resources are closely aligned.</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>10. My institution's business objectives drive our technology deployment and investment.</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
</tr>
</tbody>
</table>

**TOTAL SCORE:** __________
Fostering Technology Human Resources

This section considers technology employees, the opportunities presented to them, and the degree of communication they have with their internal customers. Circle the number that best describes your institution. Circling "STRONGLY AGREE" implies that the entire statement is true for your entire institution. Circling "STRONGLY DISAGREE" means that no part of the sentence is true.

<table>
<thead>
<tr>
<th></th>
<th>My institution employs a talented staff with competency to determine my technology strategy.</th>
<th>STRONGLY DISAGREE</th>
<th>DISAGREE</th>
<th>NEUTRAL</th>
<th>AGREE</th>
<th>STRONGLY AGREE</th>
</tr>
</thead>
<tbody>
<tr>
<td>11</td>
<td></td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>My institution has adequate and skilled staff to effectively implement and monitor my technology plan.</th>
<th>STRONGLY DISAGREE</th>
<th>DISAGREE</th>
<th>NEUTRAL</th>
<th>AGREE</th>
<th>STRONGLY AGREE</th>
</tr>
</thead>
<tbody>
<tr>
<td>12</td>
<td></td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>My technology staff meets regularly with their business and operational counterparts within the bank to ensure effective communication.</th>
<th>STRONGLY DISAGREE</th>
<th>DISAGREE</th>
<th>NEUTRAL</th>
<th>AGREE</th>
<th>STRONGLY AGREE</th>
</tr>
</thead>
<tbody>
<tr>
<td>13</td>
<td></td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>My technology staff is encouraged to look outside the institution for new uses of technology.</th>
<th>STRONGLY DISAGREE</th>
<th>DISAGREE</th>
<th>NEUTRAL</th>
<th>AGREE</th>
<th>STRONGLY AGREE</th>
</tr>
</thead>
<tbody>
<tr>
<td>14</td>
<td></td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>My institution's technology staff is capable of assessing new technologies and determining which ones are most appropriate for my institution.</th>
<th>STRONGLY DISAGREE</th>
<th>DISAGREE</th>
<th>NEUTRAL</th>
<th>AGREE</th>
<th>STRONGLY AGREE</th>
</tr>
</thead>
<tbody>
<tr>
<td>15</td>
<td></td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>My institution offers an appealing work environment and opportunities to attract talented technology staff.</th>
<th>STRONGLY DISAGREE</th>
<th>DISAGREE</th>
<th>NEUTRAL</th>
<th>AGREE</th>
<th>STRONGLY AGREE</th>
</tr>
</thead>
<tbody>
<tr>
<td>16</td>
<td></td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>My institution continually provides our technology staff with on-going opportunities for training and education in new technologies and applications.</th>
<th>STRONGLY DISAGREE</th>
<th>DISAGREE</th>
<th>NEUTRAL</th>
<th>AGREE</th>
<th>STRONGLY AGREE</th>
</tr>
</thead>
<tbody>
<tr>
<td>17</td>
<td></td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>My institution effectively manages our technology resources.</th>
<th>STRONGLY DISAGREE</th>
<th>DISAGREE</th>
<th>NEUTRAL</th>
<th>AGREE</th>
<th>STRONGLY AGREE</th>
</tr>
</thead>
<tbody>
<tr>
<td>18</td>
<td></td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
</tr>
</tbody>
</table>

**TOTAL SCORE:** _______________
Communicating Technology Strategy

This worksheet helps determine how clearly your institution communicates its technology plans and objectives to its employees and customers. It also assesses your institution’s ability to convey its technology strategy and the importance it has on the products and services offered, and the customers that use them. Circling “STRONGLY AGREE” implies that the entire statement is true for the entire institution. Circling “STRONGLY DISAGREE” means that no part of the sentence is true.

<table>
<thead>
<tr>
<th></th>
<th>STRONGLY DISAGREE</th>
<th>DISAGREE</th>
<th>NEUTRAL</th>
<th>AGREE</th>
<th>STRONGLY AGREE</th>
</tr>
</thead>
<tbody>
<tr>
<td>19. My institution fully understands our technology plan and how it relates to the individual departments that they represent.</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>20. Each functional area (e.g., credit, branches, and operations) understands the objectives set forth in the technology plan for the other functional areas within my institution.</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>21. When a customer contacts us, our representatives can clearly explain our technology strategy and how it is deployed within the institution.</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>22. Our institution effectively conveys to our customers the technology investments we are making and why they are advantageous.</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
</tr>
</tbody>
</table>

23. Our institution understands the economic impact of our technology investments and how it affects our customers.

TOTAL SCORE: ____________________
Judging Technology Effectiveness

This worksheet helps identify your institution’s current technology, its degree of effective use, and its justification for the use of future technologies. Circle the number that best describes your institution. Circling "STRONGLY AGREE" implies that the entire statement is true for the entire institution. Circling "STRONGLY DISAGREE" means that no part of the sentence is true.

<table>
<thead>
<tr>
<th>Statement</th>
<th>STRONGLY DISAGREE</th>
<th>DISAGREE</th>
<th>NEUTRAL</th>
<th>AGREE</th>
<th>STRONGLY AGREE</th>
</tr>
</thead>
<tbody>
<tr>
<td>24. Our technology effectively meets the objectives of my institution users and customers.</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>25. Our institution can identify all of the technologies that we currently utilize.</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>26. My institution deploys technology across our business units consistent with their contribution to our institution.</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>27. My institution's technology resources are closely aligned to the goals and priorities of our lines of business.</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>28. My institution deploys technology in a way that offers our customers competitive products and services.</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>29. My institution has a successful track record for implementing new technologies.</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>30. My institution has the tools and procedures to measure the success of our technology on product profitability and customer value.</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>31. My institution is open to understanding new technologies and how their implementation can better my institution.</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>32. As new technologies are implemented, our resources, workflow, and supporting operations are modified to effectively take advantage of the new technologies.</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>33. Our institution has a process in place to measure the effectiveness and ROI of our technology investments.</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
</tr>
</tbody>
</table>

**TOTAL SCORE:** ________________
Matching Technology And Business Requirements

This worksheet assesses your institution’s ability to define its business requirements and technology specifications. A critical component of this ability is having a process in place to continually identify new requirements as well as monitor the implementation of technology solutions. Circle the number that best describes your institution. Circling "STRONGLY AGREE" implies that the entire statement is true for your entire institution. Circling "STRONGLY DISAGREE" means that no part of the sentence is true.

<table>
<thead>
<tr>
<th></th>
<th>STRONGLY DISAGREE</th>
<th>DISAGREE</th>
<th>NEUTRAL</th>
<th>AGREE</th>
<th>STRONGLY AGREE</th>
</tr>
</thead>
<tbody>
<tr>
<td>34. My institution has in place a process to capture customer and employee input to improve our use of technology.</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>35. My institution has the ability to effectively define our business requirements and support them with related technology specifications.</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>36. My institution can anticipate future requirements that may not be high priorities today.</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>37. My institution has resources that can clearly document all identified requirements and gain the concurrence of the business units involved.</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>38. My institution has a review process and procedure to approve or decline proposed technology solutions.</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>39. My institution has established a program to monitor and evaluate our Web sites’ vulnerability to attack at least annually.</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>40. My institution has established a security plan with a review and sign off by the Board of Directors.</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>41. My institution has established a privacy policy that is in compliance with Gramm-Leach-Bliley Financial Modernization Act.</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
</tr>
</tbody>
</table>

**TOTAL SCORE: _______________**
**Scoring Instructions**

To score your answers:

1. Using the number contained in the circle under each question, add the scores for each environment (worksheet). Enter this number in the space next to "Total Score."

2. Divide the "Total Score by the number of questions in each section. This will give you a score between 1 and 5. Enter this number in the space next to "Average Score." This is the average score for that environment.

3. Plot the average score on the appropriate axis of the Kiviat chart below.

4. Connect the scores for the entire environment, and then shade the enclosed area.

**SCORECARD**

<table>
<thead>
<tr>
<th>PLANNING PROCESS</th>
<th>RESOURCES</th>
<th>COMMUNICATION</th>
<th>TECHNOLOGY</th>
<th>REQUIREMENTS</th>
</tr>
</thead>
<tbody>
<tr>
<td>a. Total Score</td>
<td>a. Total Score</td>
<td>a. Total Score</td>
<td>a. Total Score</td>
<td>a. Total Score</td>
</tr>
<tr>
<td>b. Number of Questions</td>
<td>b. Number of Questions</td>
<td>b. Number of Questions</td>
<td>b. Number of Questions</td>
<td>b. Number of Questions</td>
</tr>
<tr>
<td>c. Average Score (a/b)</td>
<td>c. Average Score (a/b)</td>
<td>c. Average Score (a/b)</td>
<td>c. Average Score (a/b)</td>
<td>c. Average Score (a/b)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Planning Process</th>
<th>Resources</th>
<th>Communication</th>
<th>Technology</th>
<th>Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>8</td>
<td>5</td>
<td>10</td>
<td>7</td>
</tr>
</tbody>
</table>

**KI V I AT CHART**

The Kiviat chart below presents an assessment of your institution's technology readiness. The chart contains five axes, representing each of the five areas (questionnaires) that were assessed (1 representing a low level of readiness and 5 a very high level of readiness). Shade in the scores for each environment to get a portrait of technological culture and environment at your institution.
Tool 2: Assessing Information Security and Risk

Performing a risk assessment is critical to establishing an effective information security program. The risk assessment provides a framework for establishing policy guidelines and identifying the risk assessment tools and practices that are appropriate for your institution.

The risk assessment process can sometimes feel like a maze, with a large number of variables and seemingly endless list of possibilities. To demystify the process, we have developed a set of tools for you to rank the relative risk to your various systems and applications that house customer and other important information in your institution. The tools take you through a three-step process, consisting of completing an inventory of your applications, assessing their relative importance and the potential risk to them, and finally assigning a risk weight. You will find that each worksheet or questionnaire can be easily amended to suit the particular needs of your institution.

The Risk Assessment Process

The Guidelines at a Glance provide an effective snapshot of what your institution should consider when undergoing a thorough and proactive risk assessment. The first step in the process is to fully understand where customer and other important information is housed, who is it shared with, and who should have ultimate responsibility for the safety of that information. Completion of the customer information sharing assessment questionnaire is an effective way to establish ownership of the information and be able to chart its flow within your institution. The findings from that questionnaire will assist you in completing the larger task of looking at each of your information systems and applications and assigning a risk weight to each of them.

<table>
<thead>
<tr>
<th>Guidelines at a Glance: Evaluating the Risk Assessment Process</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Key Questions or Considerations</strong></td>
</tr>
<tr>
<td>A. Review the risk assessment program.</td>
</tr>
<tr>
<td>1. How does the institution assess risk to its customer information systems and non-public customer information?</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Key Questions or Considerations</td>
</tr>
<tr>
<td>---------------------------------</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>2.</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>2. Has the institution evaluated the risk to the entire customer information system?</td>
</tr>
<tr>
<td>3. Has the institution used personnel with sufficient expertise to assess the risks to its systems and customer information on an enterprise-wide basis?</td>
</tr>
<tr>
<td>4. Is the risk assessment part of a formal risk assessment process with timelines and milestones? If not, how will management ensure timely completion?</td>
</tr>
<tr>
<td>5. Does the institution have a process for identifying and ranking its information assets (data and system components) according to sensitivity? How does it use this process in its risk assessment?</td>
</tr>
</tbody>
</table>

B. Assess adequacy and effectiveness of risk assessment process.
<table>
<thead>
<tr>
<th>Key Questions or Considerations</th>
<th>What Your Institution Should Consider</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Does the institution identify all reasonably foreseeable internal and external threats that could result in unauthorized disclosure, misuse, alteration, or destruction of customer information or customer information systems?</td>
<td>Review for reasonableness the threats management has identified.</td>
</tr>
<tr>
<td>2. Does the institution support its estimate of the potential damage posed by various threats?</td>
<td>Review the process management uses to identify the potential risks and to assess the potential damage, if the risk is not mitigated.</td>
</tr>
<tr>
<td>3. Review the institution’s existing controls to mitigate risks. Does the institution’s analysis consider the current administrative, physical, and technical safeguards that prevent or mitigate potential damage?</td>
<td></td>
</tr>
<tr>
<td>4. Does the institution use test results to support its assessment of the adequacy and effectiveness of those controls?</td>
<td></td>
</tr>
<tr>
<td>5. Does the institution identify and prioritize its risk exposure, decide on the risks it must mitigate, and create a mitigation strategy? Is the decision to accept risks documented and reported to the appropriate management levels?</td>
<td>Review factors used to evaluate level of risks and acceptability of risk as a business decision. Assess the reasonableness of documentation used to support this decision. All risk acceptance must be supported adequately and approved by the appropriate level of management.</td>
</tr>
<tr>
<td>1. Does the institution promptly act to mitigate risks that pose the immediate possibility of material loss?</td>
<td>Risk assessments that uncover immediate risks of material loss should be traceable to prompt actions taken to mitigate those risks.</td>
</tr>
<tr>
<td>2. How does the institution demonstrate that the mitigation strategy was reviewed by appropriate officials?</td>
<td>Review documentation.</td>
</tr>
<tr>
<td>3. Does the risk assessment provide guidance for the nature and extent of testing?</td>
<td></td>
</tr>
<tr>
<td>4. Does the risk assessment include vendor oversight requirements?</td>
<td></td>
</tr>
</tbody>
</table>

The extent of your information security program should be commensurate with the degree of risk associated with the institution’s systems, networks, and information assets. For example, compared to an information-only Web site, institutions offering transactional Internet banking activities are exposed to greater risks. Further, real-time funds transfers generally pose greater risks than delayed or batch-processed transactions because the items are processed immediately. The extent to which your institution contracts with third-party vendors, a subject of Tool 4 of this Toolbox, will also affect the nature of the risk assessment program.

Performing a sound risk assessment is critical to establishing an effective information security program. The risk assessment provides a framework for establishing policy guidelines and identifying the risk assessment tools and practices that may be appropriate for the institution. Items to consider in the risk assessment process include:

1. Identifying mission-critical information systems, and determining the effectiveness of current information security programs. For example, a vulnerability might involve critical systems that are not reasonably isolated from the Internet and external access via modem. Having up-to-date
inventory listings of hardware and software, as well as system topologies, is important in this process.

2. Assessing the importance and sensitivity of information, and the likelihood of outside break-ins (e.g., by hackers) and insider misuse of information. For example, if a large depositor list were made public, that disclosure could expose the bank to reputational risk and the potential loss of deposits. Further, the institution could be harmed if human resource data (e.g., salaries and personnel files) were made public. The assessment should identify systems that allow the transfer of funds, other assets, or sensitive data/confidential information, and review the appropriateness of access controls and other security policy settings.

3. Assessing the risks posed by electronic connections with business partners. The other entity may have poor access controls that could potentially lead to an indirect compromise of the bank’s system. Another example involves vendors that may be allowed to access the bank's system without proper security safeguards, such as firewalls. This could result in open access to critical information that the vendor may have "no need to know."

4. Determining legal implications and contingent liability concerns associated with any of the above. For example, if hackers successfully access a bank's system and use it to subsequently attack others, the bank may be liable for damages incurred by the party that is attacked.

The Information Risk Assessment and Inventory will provide you with a methodology for assigning risk weights to your information systems.

The following table, put together by the Federal Reserve Board, also provides a few examples of situations where deficiencies in information technology elements potentially have a negative effect on the business risks of an organization. The table also provides possible action that an institution could take in these situations to mitigate its risks, and could serve as a template for your institution to use during its risk assessment process.

<table>
<thead>
<tr>
<th>Situation</th>
<th>IT Elements to be Considered</th>
<th>Potential Effect on Business Risks</th>
<th>Risk Mitigants</th>
</tr>
</thead>
</table>
| A bank holding company expands very rapidly via acquisition into new product lines and geographic areas. | **Management Processes:**
Lack of clear, cohesive strategies could result in dependence on different systems that are incompatible and fragmented.

**Integrity:** Unreliable information could be produced due to incompatible systems.

**Availability:** Critical information may not be available to management when needed.

**Credit Risk:** Exposure may increase to less creditworthy borrowers.

**Liquidity Risk:** Depositors may withdraw funds or close accounts due to unreliable account information.

**Operational Risk:** Controls may be inadequate to address the increase in manual interventions to correct incompatibility problems between affiliates’ systems, leading to a greater potential for fraudulent transactions. |  | • Develop a well thought-out plan for integrating acquired systems, mapping data-flows and sources, and ensuring reliability of systems. |
A bank's consumer loan division inputs erroneous entries into the general ledger system. **Integrity:** Billing errors and unwarranted late payment fees could occur due to the inaccurate loan information maintained by the system. **Reputational Risk:** Knowledge of errors could become widespread resulting in adverse public opinion. **Operational Risk:** Increased expenditures may be required to resolve accounting operations problems. **Legal Risk:** Litigation could arise because of errors in customer accounts due to processing deficiencies.

- Improve policies and procedures related to input of accounting entries.
- Ensure internal audit considers system aspects of accounting operations.

Substantial turnover occurs in bank's wire transfer department. **Security:** Security procedures could be compromised due to inadequate training and lack of qualified personnel. **Integrity:** System may not be able to provided “real time” funds availability. **Operational Risk:** Financial losses could occur due to fraud or incorrectly sent wire transfers. **Legal Risk:** Litigation could arise as a result of errors in customer accounts and fraudulent wire transfers. **Reputational Risk:** Knowledge of fraudulent or erroneous wire operations could result in adverse public opinion.

- Strengthen procedural and access controls for wire operations.
- Implement security measures such as passwords and firewalls.
- Develop and monitor appropriate audit trails.
- Provide for adequate training program and staffing levels.

**Information Sharing Questionnaire**

As part of your process of complying with the Gramm-Leach-Bliley Act’s privacy provisions, your institution may have conducted an assessment of your customer information sharing practices. If you did not, conducting such an assessment will prove beneficial to you as you refine your customer information security program.

This questionnaire has been structured for use by institutions of all sizes. As such, not all questions or sections may apply to your organization. The questions should be posed to all of your business units to determine information-sharing practices throughout your organization.

**Definitions to Use During the Self-Assessment**

- The term “nonpublic personal information” refers to personally identifiable financial information that is provided to you by a customer, results from any transaction with a customer or service performed for a customer, or is otherwise obtained by you. The fact that a person is your customer is also considered nonpublic personal information.
- The term “organization” refers to your entire bank, savings institution, or holding company.
- The term “business unit” refers to an organizational unit — whether affiliate, subsidiary, or line of business —of your organization.
• The term “customer” refers to someone who has a continuing relationship with you in which you provide personal, family or household services. (This is consistent with the definition of “customer” in the GLB Act.)
• The term “third party” refers to non-bank entities to which you outsource certain business functions or those with which you have affinity or co-branded arrangements, joint ventures, or marketing-related relationships.

How Do You Collect Customer Information?

1. What types of information do you collect from or maintain about your customers (e.g., application information, account balance or transaction information)?

2. By what means do you collect information from your customers (e.g., from applications, over the telephone or the Internet)?

3. What information that you collect from customers can be obtained legally from public sources?

4. Are certain customers provided (or do they need to be provided with) different levels of information protection, based upon business needs or regulatory requirements?

5. If you retain information on former customers or declined applicants, how do you use these data (e.g., for marketing purposes such as reacquisition of the customer or to market a different product offering)? How long is information about former customers retained?

6. Do you purchase or collect information about your customers, or about potential customers, from outside sources (e.g., outside lists, marketing companies, external databases, consumer reporting agencies)?
   a. If yes, please specify the names of these outside data sources.
   b. Describe the type of information collected.

7. Do you collect customer data or manage transactions through your organization’s website?
   a. If yes, please describe the type of information collected.

8. Do you collect customer data through a relationship with a “nonbank” or shared website (e.g., a third party provider of Internet banking services or a joint marketing effort with a strategic partner such as Excite or AOL)?

How Do You Share Customer Information Within Your Organization?

Sharing of customer information between business units within an organization is not restricted by the GLB Act (including between operating subsidiaries and affiliates). Nonetheless, the manner in which information is shared across the organization has important security considerations.

9. Other than for a customer-initiated transaction, do you collect information about current, former, or declined customers from other business units within the organization? Do you provide customer information to other units?
   a. Please specify the names of these business units.
   b. Describe the type of information collected or provided.
   c. What is this information used for (e.g., cross-marketing purposes, collections)?
10. Do you maintain a list of customers who have told you they do not want to receive marketing solicitations?

11. Is there an authorization process that other business units must go through in order to access and use your customer information?

12. Are formal agreements established with other organizational business units for customer data sharing? If so, please attach.

13. Do requests for customer lists from within your business unit go through a single point of contact? If yes, please describe where this list management function resides and who is the point of contact.

How Do You Share Customer Information with Third Parties?

Understanding the manner in which your organization shares customer information with third parties is vital to safeguarding it. A checklist of security questions to ask such third parties has been included in Tool 4.

14. Is customer information being shared between your business unit and third parties? If yes, please continue here. If not, skip to the next section.

15. Do you outsource certain business functions to third parties that have access to your customer data (e.g., data processing, billing, and customer service)? If yes:
   a. Identify each third party and type of data shared.
   b. Describe any contract provisions that address the use of customer information? Do these contract provisions prohibit the reuse of customer information and maintain the information’s confidentiality?
   c. Describe any additional controls or practices (beyond the contract) to protect customer information.

16. Do you use third parties to market your business unit’s products (e.g., mortgage brokers, online business partners)? If yes:
   a. Describe any contract provisions that address the use of customer information.
   b. Do these contract provisions prohibit the reuse of customer information and maintain the information’s confidentiality?
   c. Describe any other controls or practices (beyond the contract) to protect customer information.

17. Do you securitize any of your products or sell their servicing rights? If yes:
   a. Describe any contract provisions that address the use of customer information. Do these contract provisions prohibit the reuse of customer information and maintain the information’s confidentiality?
   b. Describe any other controls or practices (beyond the contract) to protect customer information?

18. Do you share customer information with other types of unaffiliated third parties (e.g., for marketing their products or joint marketing of financial service products)? If yes:
a. Identify each partner and type of data shared.

b. Describe any contract provisions that address the use of customer information. Do these contract provisions prohibit the reuse of customer information and maintain the information’s confidentiality?

c. Describe any additional controls or practices (beyond the contract) to protect customer information.

19. Does your bank have affinity or co-branding partners? How about loyalty programs? Do these programs involve the sharing of personal information?

20. Do you receive income for customer information provided to unaffiliated third parties? If yes:
   a. What are the names of these third parties and what is the nature of the exchange?
   b. What type of information is provided (e.g., name, address, transaction history, social security number)?
   c. Describe any other controls or practices (beyond the contract) to protect customer information.

21. Are you aware of any third parties that share your customer information with other third parties? If yes, please describe.

22. Is there an authorization process to sign on additional third-party marketing partners? If yes, please describe.

23. Are third-party marketing partners periodically audited or reviewed to validate their continued compliance with customer privacy and security requirements? If yes, how?

24. Do you acquire customers in bulk from other corporations (e.g., loan portfolio purchases, securitizations, mergers and acquisitions)? If yes:
   a. What are the names of these corporations and what is the nature of the exchange?
   b. What type of information is provided (e.g., name, address, transaction history, social security number)?
   c. Do you honor acquired customers’ existing choices regarding opt-out (if any)? If yes, how?

25. Do you provide these customers with a new opt-out opportunity? If yes, please describe.

26. Do you report information to consumer reporting agencies?

How Do You Provide Information Security?

27. Do you have written policies and procedures to manage and control information security risks? If yes, please attach.

28. Did your board approve these policies and procedures? Did the board oversee management’s implementation of the information security program, and does it periodically evaluate its effectiveness?
29. Do you have formal procedures for authenticating customers in person at a branch, through the mail, via the telephone, fax, and the Internet? If yes, please describe.

30. Do you have formal procedures to assist customers who have forgotten their password, PIN or other identification? If yes, please describe.

31. Do you use social security numbers to identify customers within your business unit?

32. Do you have controls to protect customer social security numbers beyond those controls for other types of customer data? If yes, please describe.

33. Do you provide customer social security numbers to unaffiliated third parties? If yes, please describe.

34. Do you have access restrictions at locations containing customer information, such as buildings, computer facilities, and record storage facilities?

35. Do you encrypt electronic customer information, including information while in transit or in storage on networks or systems to which unauthorized individuals may have access?

36. Do you have procedures to confirm that customer information system modifications are consistent with the institution’s information security program?

37. Do you have dual control procedures, segregation of duties, and employee background checks for employees with responsibility for safeguarding or access to customer information?

38. Do you have monitoring systems and procedures to detect actual and attempted attacks on, or intrusions into, customer information systems?

39. Do you have response programs that specify actions to be taken when unauthorized access to customer information systems is suspected or detected?

40. Do you have protection against and response programs to preserve the integrity and security of customer information due to physical hazards or technological failures?

41. Is there a single point of contact in your business unit responsible for addressing customer information practices? If so, please indicate this person’s name and phone number.

**Information and Risk Assessment Inventory (XLS)**

**Intrusion Risk Assessment and Mitigation**

Your institution has a variety of measures that can be taken to reduce the risk of intrusion to one of your applications. The following listing of major applications provides examples of some of the measure available to you, as well as actions to consider in the event of an intrusion.

1. **Core Banking System**

   Accessibility to an intrusion: Via network router and local area network.

   Measures to consider taking to reduce the risk of an intrusion:

   1) Installation of an Internet firewall.
   2) Restricted access to the mainframe command line.
   3) Restricted access to upload and download programs.
4) Restricted access to system utility programs.
5) System modem in kept off-line when it’s not in use.
6) Assignment of unique user-IDs and confidential passwords.
7) Prompt canceling of inactive system sessions.
8) Requirement to work with well-known, well-capitalized vendors.

Actions to consider taking in the event of an intrusion:

1) Disconnect Internet connection from router.
2) Disconnect phone line from modem.
3) Disconnect mainframe from router. (This will disable all terminals, except for the main console.)
4) Contact the FBI, the local police, and the primary Regulator.
5) Contact vendor for primary system.

2. Fed Line Operations

Accessibility to an intrusion: Via system server

Measures to consider taking to reduce the risk of an intrusion:

1) Use of Fed Line System security controls.
2) Separation of duties.

Actions to consider taking in the event of an intrusion:

1) Contact Regional Federal Reserve office.
2) Contact the FBI, the local police, and the primary Regulator.

3. Check Imaging and POD Operations

Accessibility to an intrusion: Via system server

Measures to consider taking to reduce the risk of an intrusion:

1) Use of system security controls.
2) Separation of duties.

Actions to consider taking in the event of an intrusion:

1) Contact the vendor
2) Contact the FBI, the local police, and the primary Regulator.

4. Internet Banking System

Accessibility to an intrusion: Via network router

Measures to consider taking to reduce risk of an intrusion:

1) The web server is kept off-site, and, managed by a professional Internet Service Provider (ISP) vendor.
2) Contract with the ISP vendor stipulates that it will have an annual third party SAS 70 audit or other audit.
3) Contract with vendor also stipulates that it will have annual third party penetration tests.
4) All audit and penetration test reports for the vendor are reviewed by management.
5) All regulatory reports for the vendor are reviewed by management.
6) The vendor must respond in writing to any critical weaknesses noted by auditor and examiners.
7) Vendor’s financial condition is monitored on at least an annual basis. More frequent monitoring will occur if the vendor starts having financial trouble.
8) Users of the system are required to use an Internet browser that has a minimum of 32-bit encryption.
9) New users of the system must authenticate their identity, prior to being allowed to enroll for the service.
10) System users that require customer service (e.g., password resetting, user-ID resetting, etc.) must authenticate their identity, prior to the service being rendered.

Actions to consider taking in the event of an intrusion:
1) Contact vendor for primary system.
2) Contact the FBI, the local police, and the primary Regulator.

5. Local Area Network

Accessibility to an intrusion: Via the router, e-mail, and local area network.

Measures to consider taking to reduce the risk of intrusion:
1) Installation of an Internet firewall.
2) Assignment of unique user-IDs and confidential passwords for the network.
3) Installation of a virus detection system, with an auto-update feature that automatically interacts with the vendor’s web site.
4) Assignment of private directories.
5) Careful control of shared directories.
6) Restricted use of Admin rights.

Actions to consider taking in the event of an intrusion:
1) Contact network support company.
2) Contact the FBI, the local police, and the primary Regulator.

6. Internet & E-mail Operations

Accessibility to Intrusion: Via the ISP, network router & e-mail.

Measures to consider taking to reduce risk of intrusion:
1) Installation of an Internet firewall.
2) Installation of a virus detection system, with an auto-update feature that automatically interacts with the vendor’s web site.

Actions to consider taking in the event of an intrusion:
1) Contact ISP.
2) Contact network support company.
3) Contact the FBI, the local police, and the primary Regulator.

7. ATM System

Accessibility to an intrusion: Via the system server.

Measures to consider taking to reduce the risk of an intrusion:
1) Use of system security controls.
2) Separation of duties.

Actions to consider taking in the event of an intrusion:

1) Contact the vendor
2) Contact the FBI, the local police, and the primary Regulator.

8. Debit Card System

Accessibility to an intrusion: Via the system server

Measures to consider taking to reduce the risk of an intrusion:

1) Use of system security controls.
2) Separation of duties.

Actions to consider taking in the event of an intrusion:

1) Contact the vendor
2) Contact the FBI, the local police, and the primary Regulator.

9. Telephone Banking System

Accessibility to an intrusion: Via the system server

Measures to consider taking to reduce the risk of an intrusion:

1) Use of system security controls.

Actions to consider in the event of an intrusion:

1) Contact the vendor
2) Contact the FBI, the local police, and the primary Regulator.

10. Teller System

Accessibility to an intrusion: Via the system server

Measures to consider taking to reduce the risk of an intrusion:

1) Use of system security controls.

Actions to consider taking in the event of an intrusion:

1) Contact the vendor
2) Contact the FBI, the local police, and the primary Regulator.

11. New Deposit and New Loan Systems

Accessibility to an intrusion: Via the system server

Measures to consider taking to reduce the risk of an intrusion:
1) Use of system security controls.
2) Separation of duties.

**Actions to consider taking in the event of an intrusion:**

1) Contact the vendor
2) Contact the FBI, the local police, and the primary Regulator.

**12. Check ordering System**

**Accessibility to an intrusion:** Via workstation PC or LAN.

**Measures to consider taking to reduce the risk of an intrusion:**

1) Use of system security controls.
2) Deactivate the auto-answer feature on the PC modem.

**Actions to consider taking in the event of an intrusion:**

1) Disconnect the phone line to the modem.
2) Contact the vendor.
3) Contact the FBI, the local police, and the primary Regulator.

**13. Workstation PCs**

**Accessibility to an intrusion:** Via workstation PC or LAN

**Measures to consider taking to reduce the risk of an intrusion:**

1) Limit the use of dial-up modems.
2) Activate the BIOS passwords
3) Activate the screensaver passwords.

**Actions to consider taking in the event of an intrusion:**

1) Disconnect the phone line to the modem.
2) Contact the FBI, the local police, and the primary Regulator.
Tool 3: Managing and Controlling Risk

A key element of safeguarding customer information is the establishment, through your institution's security policy, of the lines of authority and responsibilities regarding information security, as well as the expectations of the Board. The policy serves as the roadmap from which the rest of your customer information security program flows.

Your program itself is where the rubber meets that road. It entails setting up specific security obligations for all employees, determining access rights to customer information based upon job duties, and putting in place controls, intrusion protections, and levels of authentication to limit unauthorized access to information.

Safeguarding customer information is a process that requires the commitment of your entire institution. Each business unit should have the responsibility for being the first line of defense for the information under their control. Simply put, everyone in your institution should feel an obligation to manage and control the daily risks presented to customer data.

Writing Your Security Policy

Your written security policy, as approved by your Board of Directors, serves as the window to your security practices. The policy is an expression of your commitment to the safeguarding of customer information, as well as a statement of the specific actions you are taking as an institution to maintain information security.

Your security policy to large degree serves as the “table of contents” to your security program, with your program documentation showing that you “practice what you preach.” No one size fits all when it comes to an institution’s policy, as an institution’s practices will vary depending on its complexity and composition of services and delivery systems. At the same time, there are common characteristics to all policies.

All policies, for instance, should designate who is responsible for the development, implementation, and maintenance of the institution’s security program. The policy should also direct that management identify internal and external risks to customer information and manage and control those risks. The policy should also mandate that the institution exercise proper management of any risks to customer information as a result of the use of third party service providers, and that all employees have the appropriate skills and training relative to the nature of their position.

Institutions vary to the extent that they put additional information in their security policy regarding the specific measures that the institution takes to safeguard customer information. If you do not articulate these measures in your security policy, they will need to be spelled out in your security program documentation.

We have provided you with four sample policies with varying degrees of detail and complexity. The first sample security policy is designed for those institutions that currently do not offer Internet banking, while the other three are for those institutions that offer Internet banking and/or other electronic banking services.

Information Security Policy Sample 1
[Designed For An Institution Without Internet Banking]

Objectives

In response to Section 501(b) of the Gramm-Leach-Bliley Act, [Your Institution] has developed guidelines to establish appropriate standards relating to the administrative, technical and physical safeguards of customer records and information. These safeguards are designed to:

- Ensure the security and confidentiality of customer information,
- Protect against any anticipated threats or hazards to the security or integrity of such information,
Protect against unauthorized access to or use of customer information that could result in substantial harm or inconvenience to any customer.

This Customer Information Security Program will:

- Identify and assess the risks that may threaten customer information,
- Develop written policies and procedures to manage and control these risks,
- Implement and test the plan, and
- Adjust the plan to reflect changes in technology, the sensitivity of customer data and internal or external threats to information security.

Identification and Assessment of Risks

[Your institution] recognizes that it has both internal and external risks. Some of these risks have already been discussed in the Bank's Privacy Policy and the Bank's Business Plan. The risks identified in the Business Plan include credit risk, market risks interest rate risk, liquidity risk, operational risk, legal risk, and reputational risk. More risks are detailed in the Contingency Plan/Emergency Preparedness Plan of the Bank.

In addition to these risks, other specific areas of risk for consideration for in this policy are:

- Unauthorized access and/or use of personal customer information by means of computer and electronic data, or paper documents and files,
- Unauthorized access and/or use of personal customer information by third party vendors, and
- Unauthorized access to the data processing or telephone communication system.

Management and Control of Risks

Access to customer information via the institution’s computer information system is limited to those employees who have a business reason to know such information. Each employee is assigned a login code and password. Loan files, signature cards and other legal and paper documents and records are kept in file cabinets or vaults that are locked each night. Only authorized employees know combinations, and the location of keys.

Because we are a community-based financial institution with few employees, many employees have access to all customer files and information. This is necessary to best serve our customers. To further protect customer information, the institution rotates tasks/jobs within the institution. Paper documents contain personal identifying customer information are shredded. Since we have a “closed system” with our data processor, [IT Servicer, Inc.], these procedures minimize risk by limiting physical accessibility for customer information security.

In that our institution does not have a web page or Internet banking, we have avoided some of the threat of viruses and hackers. Anti-virus software is installed and back-ups are completed, which limit technological risk. References for new employees are checked. During orientation, each new employee will receive proper training regarding the institution’s Privacy and Customer Information Security policies and the importance of confidentiality. He or she is trained in the proper use of computer information, passwords, and codes. Training also includes controls and procedures to prevent employees from providing customer information to an unauthorized individual, including "pretext calling" and how to properly dispose of documents that contain personal identifying information.
The Privacy Policy, Privacy Notice and Customer Information Security Policy are reviewed annually with all employees. Other training is provided to protect against destruction, loss, or damage of customer information due to potential environmental hazards, such as fire and water damage or technological failures. All of this training will help minimize risk and safeguard customer information security.

Implementation, Testing, and Adjustments

[IT Servicer, Inc.] provides security reports that are reviewed to ensure that no attempt has been made by non-employees to gain access to the institution's computer information system. Also, system computer maintenance reports are reviewed to ascertain that no unauthorized changes have occurred to customer account information or personal data.

Inappropriate access to information could result in the filing of a Suspicious Activity Report (SAR), employee counseling, and/or termination. A SAR may also be filed if a bank non-employee, such as an outside intruder, or employee of a third party vendor, attempts unauthorized activity.

Service Providers

[Your institution] performs due diligence in its review of its service providers for the protection of customer information. By contract, [your institution] requires that service providers have controls in place to ensure that they and any subcontractor used by the service provider will also be able to protect customer information. The institution requests copies of audits and test result information that indicate that the service provider implements information security measures. Bank management reviews the information annually.

Assignment of Responsibility

Institution management will be responsible for the development, implementation and maintenance of the program and will assign specific responsibility for its implementation and administration. Management will review the standards set forth in this policy and recommend updates and revisions as necessary. It may be necessary to adjust the plan to reflect changes in technology, the sensitivity of customer data and internal or external threats to information security.

The Institution will approve the Customer Information Security Policy initially and annually.

The board of directors approved and adopted this policy on ________________.

Information Security Policy Sample 2
[Designed For An Institution With Internet Banking]

The board of directors of [your institution], recognizing the importance of the interagency guidelines establishing standards for safeguarding customer information to our institution, hereby adopts the following Customer Information Security policy.

There are many critical elements of this policy, including assessing risk, assigning accountability, active board management, testing and monitoring, continuing training and education, developing internal controls, and planning for future developments.

Assessment Of Risk To The Bank

The board of directors directs management to take the necessary steps to identify internal and external threats that could result in unauthorized disclosure, misuse, alteration, or destruction of customer information or customer records.

Risks may include, but are not limited to:

- Unauthorized access of information by someone other than the owner of a consumer account
Compromised system security as a result of system access by a computer hacker

Interception of data during transmission

Loss of data integrity

Physical loss of data in a disaster

Poor audit trails

Errors introduced into the system

Corruption of data or systems

Lack of transaction completeness and documentation

Unauthorized access of information by employees

Unauthorized telephone requests for information

Unauthorized access through hardcopy files or reports

Unauthorized transfer of information through third parties

The board recognizes that this may not be a complete list of the risks associated with the protection of customer information. Since technology growth is not static, new risks are created regularly. The board directs senior management to identify risks to the bank by using a process of monitoring, measuring, and identifying risks for which the bank must be prepared. Department heads must develop a risk assessment in their areas and implement a written program for safeguarding customer information. These assessments and programs will be reviewed and updated not less than annually.

The board designates the senior bank security officer as responsible for assessing the risks associated with unauthorized transfers of customer information and implementing procedures to minimize those risks to the bank. The board also directs internal audit personnel to conduct reviews of all areas that have access to customer information to assess the internal control structure put in place by bank management and to verify that all bank departments adhere to the general requirements of this policy.

Elements Of Customer Information Security Plan

The board of directors directs management to include at least the following elements in its customer information security plan.

Risk Assessment

Each department head will prepare a written risk assessment for his or her area to be submitted to senior management that identifies the internal and external threats of unauthorized disclosure of customer information. This assessment will be updated and submitted to senior management annually on July 1.

Internal Routines and Controls

Bank management, together with internal audit personnel, will develop a range of comprehensive system reviews and tests to validate the controls incorporated into each bank area to protect customer information. Furthermore, management is instructed to train all users on the need to adhere to control standards.
Management Supervision and Internal Controls

Senior management and the board of directors will be actively involved in decision-making processes to contain risks effectively. The board will review, approve, and monitor new products and delivery channels that may have a significant impact on the bank’s protection of customer information. The Board of Directors appoints ______ as the Consumer Data Security/Privacy Coordinator. The Consumer Data Security/Privacy Coordinator will be expected by the board to critically evaluate the design, operation, and oversight of the plan. The Coordinator will also be responsible for assessing current and developing industry standards in determining whether to implement specific technologies. Furthermore, the board directs management to report annually on the steps it has taken to assess the risks to the security of our customers’ nonpublic personally identifiable information.

Service Providers

Due to the specialized expertise needed to design, implement, and service new technologies, vendors may be needed to provide resources that the bank is unable to provide on its own. However, the board and senior management remain responsible for the performance and actions of these vendors while they are performing work for the bank.

Service Provider Agreements

The board directs management to ensure that a clause is included in all contracts with service providers, which requires service providers to implement appropriate measures to safeguard customer information and to refrain from sharing any customer information with any other party. Current provider contracts without a privacy clause are valid until July 2003. However, management is directed to maintain a tickler file to ensure that as contracts come up for renewal, a privacy clause is included. Furthermore, all service provider contracts must include such a clause by July 1, 2003.

Due Diligence of Service Providers

Management is directed to determine the adequacy of the service provider’s system of safeguarding information based on the type of service provider and the service provider’s independent standards. Depending on the service provider, management may wish to review the service provider’s audits, summaries of its test results for security, or other internal and external evaluations.

Expertise and Training

It is critical to the success of a customer information protection program that key employees and vendors have the expertise and skills to perform necessary functions and that they are properly trained. The board authorizes senior management to allocate sufficient resources to hire and train employees and to ensure that adequate backup exists if key people leave. Training may include technical course work, attendance at industry conferences, and participation in industry working groups, as well as time allotments for appropriate staff to keep abreast of important technological and market developments.

All bank employees will be trained at least annually regarding the bank’s policies and procedures for safeguarding customers’ personally identifiable information. Management is also directed to keep documentation of this training for review by auditors and examiners.

Information Security Policy Sample 3
[Designed For An Institution With Internet Banking]

Directive

Management shall, through an effective Information Security Program (the Program):

- Assure the security and confidentiality of customer records and information as well as the proprietary records and information of the bank;
Protect against any anticipated threats or hazards to the security or integrity of such records and information; and

Protect against unauthorized access to or use of such records or information that could result in substantial harm or inconvenience to any customer or the bank.

The Program shall use appropriate administrative, technical, and physical safeguards to protect customer records and information as well as the institutions own proprietary information.

Additionally, the Program shall meet standards mandated by The Interagency Guidelines Establishing Standards for Safeguarding Customer Information (Guidelines) issued pursuant to section 39 of the Federal Deposit Insurance Act (section 39, codified at 12 U.S.C. 1831p-1), and sections 501 and 505(b), codified at 15 U.S.C. 6801 and 6805(b), of the Gramm-Leach-Bliley Act.

Responsibility and Reporting

The Chief Information Officer (CIO) is assigned primary responsibility for the development, implementation, and maintenance of the Program. To assist, the CIO may convene a committee of other managers from various divisions or departments of the bank, including Operations, Lending, Retail, and Compliance. At least annually, the CIO will report to the Board of Directors the overall status of the Program. The report shall discuss material matters related to the Program, addressing issues such as: risk assessment; risk management and control decisions; service provider arrangements; results of testing; security breaches or violations and management's responses; and recommendations for changes in the Program.

Identifying Risks

Management shall identify the reasonably foreseeable internal and external threats that could result in unauthorized disclosure, misuse, alteration, or destruction of information or information systems. Further, management shall develop and implement procedures and other controls that take into account the likelihood and potential damage of these threats.

Managing and Controlling Identified Risks

Management shall develop, implement, and maintain the Program to control the identified risks, commensurate with the sensitivity of the information as well as the complexity and scope of the bank’s activities.

Management has, as of today, identified the following security measures appropriate for the bank and either has or will shortly adopt those measures that management concludes are appropriate. Testing methods are also listed.

<table>
<thead>
<tr>
<th>Control</th>
<th>Purpose/Description</th>
<th>Bank Policy or Procedure Cross-Reference</th>
<th>Testing</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access controls on customer information systems</td>
<td>Includes controls to: Authenticate and permit access only to authorized individuals and Controls to prevent employees from providing customer information to unauthorized individuals who may seek to obtain this</td>
<td>The following Bank policies and procedures address controls on access: • PC/LAN Security Policy • Internet/Email Policy</td>
<td>Review by Outside Audit Firm of Firewall and On-Line Banking – last conducted ______. Outside Audit Firm annual review of Internal Security and Controls. Annual penetration testing by third party (name)</td>
</tr>
<tr>
<td>Control</td>
<td>Purpose/Description</td>
<td>Bank Policy or Procedure Cross-Reference</td>
<td>Testing</td>
</tr>
<tr>
<td>---------</td>
<td>------------------</td>
<td>-----------------------------------------</td>
<td>---------</td>
</tr>
</tbody>
</table>
| Security Measures | information through fraudulent means. | • Firewall Policy  
• Network Security Administrator’s Procedures  
• Ethics and Employee Conduct for Personal Use of DP Resources  
• CBS Administrator Procedures | them). |
| Encryption of electronic customer information | Includes information while in transit or in storage on networks or systems to which unauthorized individuals may have access. | The following provide methods of encryption of electronic customer information:  
• SSL technology for on-line banking  
• PGP password procedures for internal communications  
• The use of Cisco routers on data | During the annual Outside Audit Firm Controls Review audit, the SSL connections will be tested along with a review of emails for PGP usage. |
| Customer information system modifications | Procedures designed to ensure that customer information system modifications are consistent with the bank’s information security program. | Change control procedure for LANs, etc., to be added to PC/LAN Security Policy and Firewall Policy | Outside Audit Firm will review during the annual Controls Review Audit. |
| Monitoring systems and procedures | To detect actual and attempted attacks on or intrusions into customer information systems. | Net Prowler  
Monthly Log Reviews by Network Security Administrator | The annual Outside Audit Firm audit of I.S. Controls will review the log sheet of the Network Security Administrator showing what servers were reviewed and when the reviews occurred. |
| Response programs | That specify actions to be taken when the bank suspects or detects that unauthorized individuals have gained access to customer information systems, including appropriate reports to regulatory and law enforcement agencies. | Added to Firewall Policy (date) | The Network Security Administrator will update the response procedures. |
Service Provider Oversight

Management shall exercise appropriate due diligence in selecting service providers. When applicable, contracts with service providers shall specifically require them to protect the security, confidentiality, and integrity of all customer information that is under their control. Contractual performance shall be monitored.

Training

Appropriate initial and periodic ongoing training shall be provided to all associates who carry out policies and procedures adopted within the Program. The Training Department shall maintain records of all such training.

The Institution will approve the Customer Information Security Policy initially and annually.

The board of directors approved and adopted this policy on ________________.

Information Security Policy Sample 4
[Designed For An Institution With Internet Banking]

Customer information is a valuable asset. People trust their financial institutions to keep their personal financial information confidential. Financial institutions are required by law to have policies and procedures that protect against accidental, or intentional, misuse of the information.

The board of directors at [your institution] is committed to preserving and protecting customers’ information. To that end the directorate developed this Information Security Policy.

Security Objectives

The Information Security Program at [your institution] is designed to ensure that the following security objectives are met:

1. Customer information will be kept secure and confidential. The institution will implement a series of controls that help safeguard information from unauthorized viewing by non-bank personnel. Also, information about our customers will not be sold, exchanged, are given away without their prior written consent.

2. Known and anticipated threats to the institution’s Security Program will be documented, along with the measures taken to minimize the likelihood of the threats occurring.
3. Management will be proactive in searching for new threats to the institution’s Security Program. Specifically, it will attend seminars and training classes on how to protect customer information. The bank will also have an annual review of its information technology operations by a qualified third party.

**Working with Independent Service Providers**

In all instances, the institution will receive a written statement from the Service Provider where they attest to having a Security Program that meets the security objectives outlined in this policy. If the Service Provider refuses to provide such a statement, the service contract will be abrogated. (Note: contracts currently enforce are excluded from this requirement, unless the contract expires subsequent to July 1, 2003. Contract expiring subsequent to this date will be amended to stipulate that suitable security procedures will be maintained.

**Threats to Security Controls**

This portion of the policy identifies potential threats to [your institution’s] Security Controls, and what management has done to address them.

**Threat #1: Confidential customer information could be stolen.**

Measures taken to control threat:

1. All discarded reports and other confidential information is securely stored until it can be destroyed.
2. Employees will secure all reports and documents in their possession, prior to leaving for the day.
3. The ability to download data from the bank’s system is restricted to those few employees that have a need to do so.
4. Access to the mainframe computer is restricted through the use of system passwords and an automatic canceling of idle system sessions.
5. Access to personal computers is restricted through the use of screensaver passwords and basic input/output system (BIOS) passwords.
6. Personal computers and electronic media that are removed from service are reformatted prior to disposal.
7. A criminal background check is ran on all potential new employees, prior to them being hired.

**Threat #2: Customer data could be maliciously destroyed.**

Measures taken to control threat:

1. To protect against external hackers, the institution has installed an Internet firewall and virus detection software.
2. The virus detection software is updated as often as daily, via an auto-update feature that interacts with the vendors web site.
3. The institution’s IT manager checks each month, to see if there has been an update for the firewall software. All new updates are installed.
4. To protect against internal hackers, the institution limits access to “Command Line Instructions” for the mainframe computer.
5. All data files for the primary bank systems are backed-up daily and stored off-site.

**Threat #3: Unauthorized transactions could be posted to a customer’s account.**

Measures taken to control threat:

1. The security system that’s incorporated in the primary banking system is used to enforce a separation of duties.

2. All on-line posted transactions are independently reviewed, the day after they occur.

3. Access to dormant accounts is strictly limited.

4. The ability to change name and address information is strictly limited.

5. There is an independent review of newly issued and modified ATM and debit cards.

6. Wire transfer transactions are executed under dual control.

7. In most instances, customers must come to the institution to initiate a wire transfer transactions. The few transactions that are allowed to be remotely initiated are confirmed with a recorded call-back.

8. ACH files must be delivered to the bank electronically, or, delivered by someone who has transaction authority for the account.

**Threat #4: Password integrity could be compromised.**

Measures taken to control threat:

1. All employees are assigned individual user-IDs.

2. All employees select their own system passwords.

3. The system forces employees to select passwords that are hard to guess.

4. The system forces employees to change their passwords every 45 days.

5. The system prohibits employees from repeatedly using the same password.

6. Management is aware of the risk associated with “keyboard capture programs”. All PCs that suddenly begin to malfunction will be checked for such programs.

**Threat #5: Customer data could be lost due to a catastrophic event.**

Measures taken to control threat:

1. The master files are backed-up each night, and the backup files are stored off-site.

2. The institution has two (2) off-site methods for restoring the system.

3. The off-site storage location is far enough from the bank to minimize the risk that one catastrophe will destroy both the primary and backup data files.

4. The institution uses a high-quality brand of tape media, and replaces the tapes once a year.
Reporting Attempted or Actual Breaches of Security

All breaches and attempted breaches of the institution’s security controls will be reviewed to the appropriate legal authorities, via a Suspicious Activity Report.

The security officer shall also report all material breaches and attempted breaches to the board of directors.

Review and Revisions of Security Program

The chief operating officer (COO) is responsible for maintaining this policy and ensuring compliance. The Security Policy will be reviewed and revised annually by the board of directors, or its appointed committee.

Testing

Testing is necessary to validate that equipment and systems function properly and produce the desired results. Each department should perform ongoing assessments to ensure that bank personnel follow written procedures for customer information security.

Furthermore, all internal and external audits should be modified to include appropriate tests for ensuring that the privacy of our customers’ nonpublic personally identifiable information is safeguarded. The board directs management to report the results of such tests annually or more often as determined by each department’s risk assessment and written program.

Contingency Planning and Business Continuity

The risk of equipment failure and human error is possible in all systems. System failures and unauthorized intrusions may result from design defects, insufficient system capacity, natural disasters, inadequate staff training, or uncontrolled reliance on vendors. This subject is discussed at length in the bank’s disaster recovery plan.

APPROVAL

The board of directors approved and adopted this policy on ________________.

Setting Employee Responsibility

Policy Statement

[Your Institution] has implemented basic security policies and controls that govern end user computing operations, and management has the authority to evaluate the risks associated with end user computing. The purpose of this policy is to establish general guidelines for maintaining an end user computing environment within the bank that is controlled, consistent, and secure and that will enhance the productivity of end users. The board intends that the institution adhere to the guidelines set forth in the Joint Interagency Policy Statement on End User Computing Risks issued January 25, 1988. The board of directors adopts the following policies, standards, and controls as the bank’s end user computing policy.

End User Computing Policy And Procedure Responsibility

The board of directors delegates the day-to-day management of the use of microcomputers to the functional managers. They are responsible for ensuring that their employees adhere to the bank’s policies and procedures.
End User Computing Committee

The board appoints the following staff members to the end user computing committee. The purpose of this group is to assist bank management in developing and implementing policies and procedures for the end user computing environment and for reviewing these policies and procedures for feasibility, enforceability, and usability.

Information Systems Department

The information systems department is responsible for supporting and coordinating the day-to-day operation of the end user computing environment in a manner that is consistent and in compliance with the approved policies and procedures. Additionally, the information systems department should monitor and review the activities of end users to ensure that they are adhering to the institution’s microcomputing policies and procedures.

Internal Audit Department

The internal audit department is responsible for conducting periodic reviews of the end user computing environment to ensure that policies and procedures are adequate to properly control the environment and that all end users consistently follow these policies and procedures.

The internal audit department also has the responsibility to evaluate the level of compliance with the institution's end user computing standards, policies, and procedures and to report any discrepancies to the appropriate department manager for correction and enforcement and to the board of directors through the audit committee in their regularly scheduled reports.

The internal audit department will be available to management, users, and the end user computing committee to provide input and recommendations in certain circumstances, including, but not limited to, the following:

- Purchase of new software
- Automation of procedures
- Access control issues
- Termination of employees
- Development and testing of systems/procedures
- Suspicions of fraud or misuse of software and/or hardware
- Implementation of new controls and/or testing

Acquisition of Hardware and Software

The acquisition of all hardware, software, and peripherals must be properly justified and must comply with the institution's capital expenditure policies.

- All acquisitions, installations, and implementations require review and coordination by the information systems department and approval by the appropriate department executive(s).
✓ Acquisitions of local area networks (LANs) or more complex systems may require a feasibility study or evaluation prior to the approval of the acquisition. The end user computing committee will determine any additional requirements needed for the acquisition of more complex systems.

✓ The purchasing department will acquire all approved microcomputer (PC) hardware and software.

✓ The information systems department will maintain a complete inventory of hardware, software, and peripherals.

✓ All department systems will be equipped with standardized hardware and software. The end user computing committee will be responsible for reviewing and determining appropriate standardized hardware and software to be used by bank personnel.

Licensed Use of Packaged Software

Employees are required to read and comply with commercial software license agreements. Managers must be certain that employees understand that modifying, selling, or duplicating commercial software packages is illegal and expressly against the Bank’s policy. The bank may be held liable for anyone illegally obtaining or copying commercial software. Civil damages for the unauthorized copying or use of software can be $50,000 or more, and criminal penalties can include fines and imprisonment. Duplicating software includes but may not be limited to the following:

✓ Making a copy of a software program from the employee’s hard drive or from a diskette.

✓ Using the master diskette on an employee's home computer when the software is already installed on one of the bank’s computers.

✓ Installing software that currently resides on an employee’s home computer on a bank computer.

✓ Receiving an upgrade for a software package and installing the version on a different computer.

✓ The information systems department must review and audit any public domain software (e.g., Internet software) prior to installation on any bank-owned microcomputer.

Physical Protection and Security of Hardware/Software

Managers in each user area are responsible for proper and adequate physical security and protection of the hardware and software assigned to their departments. Department managers are responsible for developing and implementing appropriate physical security controls and protection of hardware and software and for ensuring compliance with established physical security policies. In addition, department managers are responsible for the following:

✓ Ensuring sensitive reports and information are properly safeguarded and disposed of in a proper manner.

✓ Assessing their department’s physical control needs and implementing controls necessary to ensure proper security and protection.

✓ Monitoring and maintaining control over the use of laptop microcomputers.

✓ Maintaining inventories of hardware and software and periodically auditing these inventories.

✓ Securing the work areas housing microcomputers.

✓ Assessing the need for locks and keys.
Establishing proper housekeeping rules.

Maintaining adequate environmental controls.

Training users on proper use and care of microcomputers.

Although ultimate responsibility for the physical protection and security of hardware and software rests with the department manager, each user is responsible for the physical security and protection of his or her own microcomputer. In addition, end users are responsible for the following:

- Abiding by all housekeeping policies established by management;
- Keeping a maintenance list identifying all maintenance done to their equipment;
- Securing any laptop microcomputer while in their possession;
- Being aware of and reporting any suspicious individuals or activity to management and
- Ensuring that all software is backed up and maintained in a secure area.

Restricted Access to Data and Software

It is the policy of the Institution to protect the processing, storage, and use of data on microcomputers, LANs or wide area network (WAN) systems based on the level of the data’s sensitivity and value to the bank. Each department manager will establish and implement proper and adequate access controls to restrict access to data and software. This is to prevent unauthorized access that could result in confidential data being accessed, improper loading of software posing the risk of viruses and use of unauthorized software, and improper downloading of programs and files that could result in unauthorized copying.

Misuse of corporate data will be reported to management and the board of directors through appropriate channels.

Each department is responsible for identifying and establishing the proper procedures to ensure that hardware, software, and documentation is adequately backed up to ensure timely recovery in the event of a disaster. The department manager will perform a risk assessment of each department to determine the impact that loss of data would have on the institution due to the following reasons:

- Incorrect management decision
- Improper disclosure of information
- Fraud
- Financial loss
- Competitive disadvantage

Based on the results of the risk assessment, each department manager will be responsible for ensuring that appropriate microcomputer backup procedures are included in each department’s respective section of the disaster recovery plan for [Your Institution].
Data Integrity

Each department manager is responsible for implementing security measures and controls to ensure that all data are adequately evaluated, tested, and validated prior to transfer or release. This includes, but is not limited to, data that:

- Reside on microcomputers, LANs, and WANs and are downloaded or uploaded to the mainframe or to another system.
- Reside on a microcomputer from which critical business decisions are made and/or financial reporting for the bank is based.

Each department is responsible for developing and maintaining a list of all sensitive data and of programs used to process the data. The manager or supervisor of the department is responsible for updating the information and communicating the information to employees.

Virus detection software will be installed on each microcomputer in the bank to help ensure that no viruses are introduced into the bank’s systems.

Program Development, Documentation, and Testing

All developed software, applications, and programs must be fully tested and adequately documented before becoming part of a system that processes the institution’s data.

Prior to the development of any new software application or program, the end user computing committee will review the request for the new application or program and perform a cost/benefit analysis.

Managers are responsible for overseeing new projects and ensuring management control of the development process. Management control will encompass all phases including the initial development phase, development of appropriate data editing controls, proper input/output controls, report design, adequate testing, and documentation.

Training And Support

The board of directors understands that the increase in microcomputer use requires that employees are properly trained and informed on the policies and procedures endorsed by the institution with regard to end user computing. The ability of employees to enter, move around, and leave the institution with ease increases the risk to the bank. Therefore, management and the board plan to address these issues through policies, education, and training of users on security and use of microcomputers.

The institution will provide end user computer training to all employees. All users will be trained before they use institution-owned hardware and software. The training department of the institution is responsible for developing end user training materials and providing information and classes for all employees. Training will cover the bank’s policies and procedures relating to end-user computing. The programs developed will increase employees’ awareness about microcomputer security risks and vulnerabilities and the appropriate preventive controls. The training department will maintain documentation concerning training of all employees for review by department managers, internal audit, the board of directors, and regulators.

The board of directors approved and adopted this policy on (date).

Cybersecurity Checklist

1. Minimize external exposure by minimizing Internet access and connectivity. This includes:
   a. Distinguishing between convenience access and essential business access. Convenience access can be identified as such services as mail lists, traffic and weather advisories, PointCast, multicast,
instant messaging, etc. These services automatically open Internet access providing an access point into your network that can be exploited;

b. Consider opening and closing connections as needed rather than leaving services up continuously; and

c. Removing Internet access from those employees who may not need it for business purposes.

2. Review security policies and ensure that they are current. More importantly, ensure that they are fully implemented, managed to, and vigorously enforced. The corporate world is full of companies that have very well thought out, carefully crafted policies that are never implemented.

3. Ensure all current service-level and security patches have been installed on operating systems and software, including anti-virus updates.

4. Enhance the review and monitoring of all critical system logs for suspect activity and consider implementing an intrusion detection system.

5. Revisit your firewall configurations and rules to ensure that unnecessary ports and services are turned off and that access control is tightly managed.

6. Considering curtailing remote access by employees, business partners, customers and consultants to essential business.

7. Consider changing passwords for all super-user or power IDs such as Root, dbadmin, application manager IDs, etc. especially if that information has become widely shared.

8. Revisit access control lists to ensure that access to critical functions and resources is limited.

9. Contact your Internet Services Provider (ISP) to discuss what measures they are taking to ensure the security and reliability of the services they are providing you.

10. Ensure all critical systems are regularly backed up and actual systems recovery procedures have been tested.

11. Consider an incident response plan for addressing actions to be taken should a debilitating cyber incident/event occur affecting your business. Review your existing plans and determine who within your company has the authority to make decisions and to take action.

Information Security Access Assessment

Branch #________________

Date _______________________

A. EMPLOYEES:

1. List all new employees and their positions that have been in your office since the last Information Security Access Assessment. Indicate if they have signed the Employee Acknowledgement to the Employee Guide to the Information Security Program:

<table>
<thead>
<tr>
<th>NAME</th>
<th>POSITION</th>
<th>Acknowledgement Signed?</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
2. Have the above employees been granted access to customer information at a level appropriate for their position?
   - Yes
   - No
   Please explain any "No" answers:

3. Has the access level been changed for any employees in the last 6 months:
   - Yes
   - No
   Please explain any "Yes" answers:

B. CUSTOMER INFORMATION

1. Is customer information kept in a secure area at night such as the vault, a locked cabinet, drawer, or locked office? (Customer information includes reports, loan files, signature cards, account documents, and any other item that contains confidential customer information.)
   - Yes
   - No
   Please explain any "No" answers:

2. During the day, is customer information kept where an unauthorized person cannot easily view or take such information?
   - Yes
   - No
   Please explain any "No" answers:

3. In the “Platform” area, are password-protected screensavers used to prevent screen information from being accessed if an employee is away from his or her desk?
   - Yes
   - No
   Please explain any "No" answers:

4. Is any confidential information left in the trash at night instead of being placed in the shred bin?
   - Yes
   - No
   Please explain any "Yes" answers:

5. Do all employees place shred items into the shred bin at the end of the day?
   - Yes
   - No
   Please explain any "No" answers:

C. PASSWORDS AND LAPTOPS

1. Are passwords kept in a secure location? (Passwords should NOT be placed on or near the computer workstation either on the monitor, underneath the keyboard, next to or near the computer.)
2. Are employees instructed NOT to use a password that is easily guessed? *(Examples of easily guessed passwords include employee names, the name and/or number of the branch, or an easy series of letters or numbers such as 1111, 12345, abcde.)*

   
   Please explain any "No" answers:

3. Are all laptops kept in a secure location at night? *(Laptops should NOT be left in an unlocked location such as a desktop or unlocked drawer unless it is inside of a locked office.)*

   Please explain any "No" answers:

**D. NEW ACCOUNTS, PRETEXT CALLING, & UPDATING CUSTOMER INFORMATION**

1. Are New Accounts personnel advising customers on the use of the Automated Calling Center?

   Please explain any "No" answers:

2. Do they advise customers to change their PIN the first time they use the system?

   Please explain any "No" answers:

3. Are they giving the Privacy Disclosure brochure to all new CONSUMER account customers?

   Please explain any "No" answers:


   Please explain any "No" answers:

5. Do all personnel have an understanding of what Pretext Calling is? *(See the Employee Guide to the Information Security Program. This should be covered periodically during staff meetings.)*

   Please explain any "No" answers:

6. Do employees know how to properly identify customers before giving out information? *(This should be covered periodically during staff meetings.)*

   Please explain any "No" answers:

7. Do employees know NOT to give out customer information just because the caller states they are an attorney or law enforcement? *(All such calls should be referred to a supervisory level person and, if necessary, to Operations Support. Attempts at Pretext Calling may require the filing of a Suspicious Activity Report.)*

   Please explain any "No" answers:
8. When an address change is requested, is the customer's identity verified before the address change is made?

- Yes  - No

Please explain any "No" answers:

9. When customer information is entered or changed on ITI, is there an independent call-back to verify the information was entered accurately?

- Yes  - No

Please explain any "No" answers:

I certify that I have reviewed the Information Security practices in this branch office and have reported the findings in this Information Security Access Assessment – Branch Office Assessment.

<table>
<thead>
<tr>
<th>Customer Service Manager - Signature</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Business Center Manager - Signature</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Remote Access Security Tips**

All institutions are feeling pressure to use new forms of remote access to help their branches and other offices stay better connected. Often that mandate has been interpreted to mean "any time, any where" access to our core business computer systems. Poorly implemented remote access techniques can have devastating effects on the viability of your business should access be gained by competitors, criminals, or vandals.

Listed below are some safeguards your institution should consider if you are either enabling or expanding the use of remote access.

1. Develop a Remote Access policy that specifically states:
   a. Who will be permitted access to the internal systems from remote locations, e.g.,
   b. What restrictions apply, e.g., do not connect a computer 'shared' by family members, roommates, or others not permitted access to corporate systems; time of day; day of week, etc.
   c. The Authentication techniques to be used.

2. Implement one-time passwords to reduce your exposure to 'sniffing' exploits.

3. Consider the sensitivity of the system or specific information being accessed. If the information is worthy of protection while stored in the host computer (access control), it is worthy of protection in transit (encryption), and it should be protected while on the remote system (access control).

4. Implement a procedure to protect the company should a laptop computer be stolen (file encryption).

5. Users who require remote access to your systems from a fixed site, e.g., home offices, will soon be establishing connections using high-speed services such as DSL and cable services. Be very careful in your consideration of these services as they can pose a significant security exposure to your company. Consider:
a. Implementing a policy requiring personal firewalls be installed on every PC using broadband (DSL/cable) connections to the corporate systems.

b. The use of VPN connections in conjunction with your remote access services.

6. In all cases, be certain to include your company's Help Desk in any and all plans involving Remote Access services. You can expect users to contact the Help Desk for assistance when they are experiencing difficulty. The Help Desk will require training to ensure they are able to provide proper user support services.

7. Consider implementing a system to help authenticate persons contacting the Help Desk seeking assistance in gaining access to your corporate computer systems. The technique of using the Help Desk is known as Human or Social engineering and it is widely used to gain unauthorized access to computer systems. Effective authentication techniques include:

a. Various password generating tokens

b. Voice recognition technology

8. Challenge and Response systems wherein the user must cite the correct response when asked a predetermined question. If the person is unable to do so, the Help Desk has a specific right to question the validity of the request for access.

9. Whatever system is implemented to support your company's remote access requirements, ensure the system is managed by a qualified (trained) systems administrator and ensure the system log files are reviewed daily.

**Authentication Practices**

Authentication, the function of verifying the identity of persons seeking access to information systems and/or electronic banking services, is a high-profile element of safeguarding customer information. There are a variety of authentication tools and systems in use today within the banking industry. These include user passwords, personal identification numbers (PINs), digital certificates using public key infrastructure (PKI), smart cards, tokens and other types of physical devices, and biometric identifiers. The degree of security afforded by each of these tools/systems varies and is evolving as technology changes.

Authentication methods generally fall into one of three basic categories or factors:

- Something the user knows (e.g., password, PIN);
- Something the user possesses (e.g., ATM or smart card, security token); or
- Something the user is (e.g., biometric characteristic, such as fingerprint or retinal pattern).

Authentication systems that involve more than one of these factors are typically more difficult to compromise than single-factor systems. Implementation and maintenance of multi-factor systems typically require greater financial and administrative resources. Consequently, an efficient authentication system is one in which the associated resource costs are commensurate with the sensitivity and criticality of the system/services being protected. Further, the success of a particular authentication method depends on more than the technology itself and the proper implementation of the technology. It also depends on the adoption of and adherence to appropriate control policies, procedures, and standards. Finally, an effective authentication method should have user acceptance, reliable performance, scalability to accommodate growth, and interoperability with existing and planned IT systems.
The Federal Financial Institutions Examination Council (FFIEC), issued Supervision and Regulation Letter SR 00-20 dated August 15, 2001. This mailing distributed the FFIEC’s guidance paper entitled “Authentication in an Electronic Banking Environment” dated August 8, 2001. This guidance document specifically addresses authenticating customers accessing an institution’s computer systems via the Internet, yet the principles discussed also apply to authenticating bank employees and third-party vendors, suppliers, and contractors attempting to access any bank-owned data and/or information system.

The guidance also applies whether the subject data or information systems are maintained in-house by the bank or housed at external data processing service providers.

The FFIEC authentication guidance addresses four elements of an effective authentication system relative to electronic banking systems: risk assessment; customer verification during account origination; transaction initiation and authentication of existing customers; and monitoring and reporting.

**Risk Assessment**

The implementation of effective authentication methods starts with management’s assessment of the risk posed by the institution’s electronic banking systems. The risk should be evaluated in light of the type of customer (e.g., retail or commercial), the transaction capabilities available, the sensitivity and criticality of the stored information to both the bank itself and the customer, and the size and volume of transactions. The authentication method implemented for a specific electronic application should be appropriate and commercially reasonable relative to the reasonably foreseeable risks in that application.

From an enterprise-wide perspective, because institutions’ information systems and product mixes change over time, management is expected to periodically conduct additional risk assessments to determine whether modifications are needed to maintain commercially reasonable authentication systems.

**Customer Verification During Account Origination**

In an electronic or online banking environment, the use of and reliance on traditional forms of paper-based authentication (face-to-face presentation of an individual’s drivers license, etc.) is generally not feasible. Alternative methods of authentication, verifying personal information, are needed. A bank can verify a potential customer’s identity by comparing their answers to a series of detailed questions against information in a trusted database for consistency (e.g., a reliable credit report); such a process is known as “positive verification.” Information provided by the potential customer may also be reviewed for logical consistency (e.g., are the telephone area code, ZIP code, and street address consistent with each other); this process is known as “logical verification.”

“Negative verification” is the process of comparing customer provided information against fraud-related databases to determine whether any of the information is associated with known incidents of fraudulent behavior. Finally, a customer’s identity can be verified through the use of an electronic credential, such as a digital certificate, issued by a trusted third party.

The ABA has recently distributed a resource guide to assist institutions in the identification and verification of account holders.

**Transaction Initiation and Authentication of Existing Customers**

Institutions are currently using a variety of methods to authenticate existing customers, including passwords, PINs, digital certificates and PKI, physical devices such as smart cards or tokens, and biometrics. Communication of customer responsibilities and recommended precautions can strengthen the reliability of such authentication methods.

**Passwords and PINs:** User IDs combined with passwords or PINs are considered a single-factor authentication technique. The degree of security provided depends on password secrecy and encryption and on password length and composition. Further, system configuration settings and password administration should be controlled via an appropriate security policy.
Digital Certificates and PKI: Due to its complexity and costs, PKI has not been widely deployed for retail-based electronic banking systems. It is an emerging tool, however, in the commercial or business-to-business sector.

Physical Devices: Devices such as smart cards or tokens are typically part of a two-factor authentication process, complemented by a password as the other factor. Authentication cannot be completed unless the device is present.

Biometrics: A biometric identifier measures an individual’s unique physical characteristics or behavior and compares it to a stored digital template for authentication. The identifier can be created from sources such as the individual’s voice, fingerprints, hand or face geometry, the iris or retina of an eye, or a signature. A biometric identifier can be used as a single or multifactor process. Although not widely used in banking for customer authentication in electronic banking applications, biometrics are increasingly used for physical access control.

Monitoring and Reporting

An effective authentication system should include monitoring or audit features that assist in the detection of fraud, compromised passwords, and unusual or other unauthorized activities. The activation, review, and maintenance of audit logs should be standard control procedures.

Adequate reporting mechanisms, including documentation trails, are needed to promptly inform security administrators when users are no longer authorized to access a particular system and to permit the timely and complete removal or suspension of user access accounts when warranted. The security administrator’s actions should be documented in activity reports and reviewed by an independent party to provide the needed checks and balances. If critical systems or processes are outsourced to third parties, clients should ensure that the appropriate logging and monitoring procedures are in place and that suspected unauthorized activities are communicated to clients in a timely manner.

Frequently Asked Questions

1. Are single-factor methods (e.g., passwords) considered adequate for institution users’ authentication to core processing systems and for customers’ authentication to electronic banking systems at community banks?

Potentially, yes, depending on appropriate verification during account origination, prudent system controls and standards relative to password administration, and effective monitoring and reporting mechanisms. The following system control settings/processes are considered integral to prudent password administration:

- Industry standards are migrating to the use of passwords with a minimum of 6 characters, comprised of a combination of letters, numbers, and special characters;
- Locking out users after an excessive number of failed login attempts – industry practice is generally no more than 5 unsuccessful attempts;
- Establishing risk-based password expiration intervals – industry practice is migrating toward no greater than 90 days;
- Implementing a secure process for password originations and resets, including forcing a password change at the next login;
- Preventing use of previously used passwords; and
- Terminating access after a specified interval of inactivity – industry practice is generally not more than 20 minutes.
2. What guidance should financial institutions be providing to system users with respect to password generation?

The security provided by a password is directly linked with its confidentiality.

Passwords should never be recorded in writing, nor shared with any other user, and the use of readily available user identifiers should be strongly discouraged (e.g. the entire or any part of a user’s Social Security number, birth date, etc.). Additionally, a password consisting of a word found in the dictionary is subject to a greater risk of compromise than one consisting of letters, numbers, and/or special characters.

3. Are FFIEC’s authentication guidelines designed to prompt community institutions to strengthen existing authentication systems?

Yes, in a general sense. Recent examination findings suggest that community institutions have generally not conducted risk assessments of the information systems deployed enterprise-wide. Risk assessments and the corresponding determination of appropriate authentication methods are needed for core application systems, network-based applications and data, microcomputer-based applications and data, and for all product/service delivery channels (e.g., ATMs, telephone banking systems, Internet banking systems). In addition, risk assessments of all systems must now consider the privacy and confidentiality of any nonpublic customer information relative to the Interagency Guidelines for Safekeeping Customer Information.

4. What are some of the key considerations of deploying digital signatures and PKI, physical devices such as smart cards or tokens, and biometric identifiers as authentication methodologies?

The FFIEC’s August 2001 guidance document, “Authentication in an Electronic Banking Environment,” provides a detailed discussion on each of these authentication methods and their associated control considerations.
As your institution's information technology needs have become more sophisticated, you have undoubtedly turned to a variety of third parties to help fulfill those needs. In such an environment, the management of these outsourcing arrangements, and the risk associated with them, has become increasingly challenging.

A recent United States Government Accounting Office Report identified three factors that are critical to successful information technology outsourcing: executive leadership, partner alignment, and relationship management. No secret here. The commitment to safe and sound outsourcing must come from the top.

Consider the interaction between you and your outsourcers a partnership, and manage it accordingly. This tool is designed to assist your institution in successfully searching for, contracting with, and managing third party vendors.

**About Outsourcing**

Today, the data processing environment of many banks consists of not only a core processing system, but also includes several separate and distinct supplemental transaction processing systems (e.g., ATM/debit card, ACH/wire transfer, telephone banking, and personal computer/Internet banking systems). Most banks have also found it necessary to deploy local-area networks, wide-area networks, and/or Internet connectivity over the past several years.

The increasing complexity and interconnectivity of all such bank-related systems, together with the difficulty of hiring and retaining staff with networking and Internet expertise, has led to increased use of third-party data processing service providers and network consultants. Simultaneously, the dynamics of the financial service provider and software vendor industries have increased with new market entrants and heightened merger/acquisition activity.

Prior to the emergence of the century date change issue in the late 1990s, regulatory examinations specifically focused on the IT environments and controls of only those banks that conducted processing of core applications (e.g., deposits, loans, general ledger, etc.) on in-house computer systems. Those institutions that outsourced their core application processing were generally subject to only cursory evaluations of their information technology controls.

Preparation for the century date change event, current industry trends, and the regulatory emphasis on risk-focused supervision, led to a change in the regulatory approach to information technology examinations in all sizes of banks. Most importantly, supervisory processes now routinely include an evaluation of IT controls and activities at all institutions, whether core processing occurs in-house or is outsourced to an external party. Furthermore, a consensus has emerged that the IT-related risks inherent in a bank's outsourced activities are substantially the same as those associated with processing activities conducted in-house. In fact, risk in an outsourced environment may be greater given the lesser degree of direct control exercisable by the client over operations at an external service provider.

These documents outline the key elements of and regulatory expectations for an institution's risk management of relationships with external servicers, vendors, and/or consultants. Briefly, these include:

**Risk Assessment:** Banks should identify and assess the key risks and the potential mitigating controls associated with the activities to be outsourced. Bank management and directorates are responsible for determining the minimum control elements that must be in place to reduce inherent risk to prudent residual levels.

**Due Diligence in Selection of Service Provider:** Banks should review/analyze the operational competence, internal control environment, and financial stability of service provider candidates during the selection process.

**Written Contracts:** A written contract or service agreement between the servicer and the client bank should be executed. It should outline the terms, responsibilities, liabilities, and service level agreements in detail commensurate with the scope and risks associated with the services to be provided. Contracts should provide assurances for performance, reliability, security, confidentiality, and reporting.
**Ongoing Service Provider Monitoring/Oversight:** Banks should implement oversight policies and practices to monitor each servicer’s controls, financial condition, and performance commensurate with the criticality of the services provided. Control information to be reviewed can include data integrity and security controls, availability controls within the servicer’s infrastructure and through its disaster recovery planning, and internal and/or external audit reports. Banks are expected to document the analyses conducted and the conclusions reached and reported to senior management and/or the directorate.

Drawing from the referenced supervisory statements, Federal Reserve examiners will employ the following principles in evaluating an institution’s vendor management practices.

An institution’s IT-related risk controls over outsourced processing should be equivalent to those needed in an in-house processing environment.

While the issued regulatory guidance directly addresses outsourced information and data processing, the risk management principles are also generally applicable to relationships with key software vendors and their products purchased for in-house use and with IT-related consultants.

The formality of vendor management practices for any particular servicer, vendor, and/or external consultant should be commensurate with the criticality of the information and/or transactions processed and the potential for impact on the institution’s traditional banking risks (i.e., credit, market, liquidity, operational, legal, and reputational risks).

An institution’s board of directors and executive management are responsible for understanding and assessing risk and for determining proper controls. While the board and management can delegate the technical implementation of IT controls to servicers and consultants, they cannot delegate the responsibility for periodic IT risk assessments, for determining prudent control policies and standards, and for monitoring the control environment. Ultimately, the client bank in a servicing arrangement retains responsibility and accountability for the integrity, security, and availability of its data.

**Frequently Asked Questions**

1. Are all banks, including those with in-house core application processing, expected to have a formal vendor management program in place?

   Yes. All banks are expected to include vendor management practices in their IT-related policies commensurate with the criticality and potential safety and soundness impact of the services outsourced. Clearly, those banks that outsource core application processing should have extensive written procedures. Those institutions with in-house core application processing should have procedures in place to evaluate the performance, stability, and viability of the core application software vendor. Further, regardless of the core application processing environment, vendor management practices should be in place for third-party servicers and/or software providers that facilitate the capture, transmission, and/or settlement of transactional inputs (e.g., ATM/debit card, ACH/wire transfer, telephone banking, and Internet banking transactions).

2. Do regulators expect that a client bank’s legal counsel review each service contract prior to execution?

   Vendor management guidelines do suggest that an institution’s legal counsel review service contracts prior to execution. Clearly, the intent of the guidelines is to ensure that both parties, particularly the client bank, understand their obligations, rights, and remedies under a proposed service contract.

   In a community bank setting, legal review by counsel is likely warranted where the proposed services are mission critical and/or have the potential to significantly impact the bank’s traditional risk elements (credit, market, liquidity, operations, legal, reputational). Other factors to consider include the complexity of the services in question and the use of standard versus custom provisions in the proposed agreement.
3. Do regulators expect service contracts to include provisions granting a client bank access to a servicer’s control policies and procedures, third-party control reviews or audits, contingency plans and test results, and financial performance data?

Vendor management guidelines clearly stipulate that client banks gather and analyze such information in reaching conclusions during the servicer selection and ongoing monitoring processes. Accordingly, it is prudent to confirm the servicer’s periodic delivery of such items under provisions of the service agreement/contract. A service provider’s refusal to address such items in a service contract, and particularly, one’s refusal to provide such items under any circumstances, should negatively influence a bank’s decision to commence or continue any service arrangements with that servicer.

Also see Appendix D-2 to Regulation H containing guidelines for the inclusion of customer information safekeeping provisions within contracts with information and data processing service providers.

4. Relative to ongoing monitoring of vendor relationships, does periodic receipt and retention of vendor information satisfy regulatory expectations?

Generally, no; simple receipt and retention of such information is insufficient to comply with regulatory guidelines. The information should be analyzed and conclusions reached regarding:

- The servicer’s compliance with the performance provisions of the service contract;
- The adequacy of the servicer’s control environment and contingency planning;
- The adequacy of and the findings from an independent review/audit of the servicer’s control environment; and
- The ongoing financial stability/viability of the servicer.

This process should be undertaken at least annually, and the conclusions reached should be documented and presented to senior management and/or the directorate.

5. Are community banks expected to participate directly in the IT-related audits and/or disaster recovery testing of their critical or significant service providers?

Generally, no; participation by every client in a servicer’s IT-related audits and/or disaster recover testing is not feasible. However, indirect participation through a national or regional user group is beneficial where applicable. Relative to an independent audit/review of a servicer’s control environment, client banks should follow-up with the servicer on any significantly adverse findings/exceptions. Relative to contingency planning, client banks should approach their own contingency planning from two perspectives. First, what actions must the client take to reestablish processing should the servicer be forced to relocate to an alternative processing site. Second, what actions must be taken should the client bank be forced to relocate to an alternative operating site.

6. What are the vendor management-related regulatory expectations for a community bank’s use of a local consultant in establishing and administrating a LAN and/or WAN?

First and foremost is the necessity for the client bank’s management to clearly define the desired purposes and functionality of the network and to establish related control policies and standards. Such definitions and standards are to govern the general deployment and configuration of network hardware and applications. They should also govern the integrity, security, and availability of network data and programs commensurate with the criticality of information and processing associated with the network. (Note: the accessibility of non-public customer information over or on the network requires that a minimum of security access controls be in place.)

Community banks’ use of local network consultants for information and advice relative to the technical aspects and potential risks of network deployment is common. Additionally, such consultants often perform
the installation of network hardware and software. However, the actual deployment and control standards
decided upon must remain the responsibility of the bank’s directorate and management team. As the
ultimate administrators of the bank’s affairs, management and the directorate cannot outsource the
responsibility and accountability for such decisions.

Recent examination experience reveals that many local network consultants prefer to provide technical and
administrative services based on an informally agreed upon cost-per-hour basis, without a written service
agreement/contract. While a written contract outlining the services to be provided is preferable, examiners
have not been highly critical of such situations and have recommended, at a minimum, that a nondisclosure
or confidentiality agreement be executed.

**Twenty-Five Steps To Service Provider Selection**

In addition to proper service provider selection being good business, the GLB Act’s Security of Customer
Information Guidelines also require examiners to determine whether the institution exercises due diligence in
selecting providers. Developing a consistent process for reviewing and selecting information technology and
other vendors for your institution enhances your ability to maintain quality and control over the process, and
also provides an audit trail. Consider taking the following steps as part of your vendor selection process:

1. Appoint a Technology Steering Committee chosen from the institution’s senior management and board
   members. Assign a Technology Management Team of key staff members to assist in the information
gathering and planning process.
2. Develop a technology strategic plan that encompasses the vendor selection process and any other
   strategic technology issues.
3. Create a Vendor Evaluation Team consisting of key senior managers and key personnel from the next
   level down in the organizational structure. This will allow representatives from all areas of the bank to
   participate in the decision-making process and identify any critical features that a vendor may lack.
4. Prepare an inventory of current technology.
5. Identify current volumes of activity by application.
6. Identify current data processing hardware and software.
7. Identify current data processing costs.
8. Survey staff to determine the critical business needs of the system.
9. Create a critical business needs document. This document should consider existing transaction
   volumes, as well as any strategic plans of the bank that might materially affect such volumes.
10. Approve a long vendor list (no more than 7-10 vendors).
11. Contact vendors and begin preliminary discussions.
12. Begin vendor marketing presentations.
13. Create an RFP from the critical business needs document.
14. Submit the RFP to the long list of vendors, allowing no more than 45 days to provide a response.
15. Receive and analyze vendors’ responses to the RFP.
16. View demonstrations of all vendors that submitted favorable responses.

17. Narrow the vendor list down to a short list of two or three. From this point forward, any vendors not on the short list should be excluded from further consideration.

18. Members of the Vendor Evaluation Team should make visits to banks using the prospective systems for additional demonstrations and check bank client references supplied by each vendor on the short list.

19. Create a detailed features and functions document and submit the document to each vendor on the short list for completion. Again, allow no more than 45 days for vendors to complete and return this document.

20. Develop a conversion plan to include testing, parallel processing, test results review and correction, contingency plans, and implementation. The plan also should address any policies and procedures that will require modification as a result of the vendor change. These modifications should be made prior to conversion. The viability of the plan will be confirmed with prospective vendors.

21. When the features and functions document is returned, it will be reviewed in detail by the vendor evaluation team. Any vendor on the short list not having a critical feature or function should be dropped from further consideration.

22. Conversion time frames and the conversion plan will be confirmed with the remaining prospective vendors.

23. Begin contract negotiations with remaining vendors. Have vendors provide sample contracts for review by the bank's attorneys.

24. Prepare a final vendor selection matrix to formally compare the features, functions, deliverables, price, and contracts of the remaining vendors.

25. Select preferred vendor, obtain senior management approval and finalize negotiations.

**Service Provider Demonstration Questionnaire**

When choosing a service provider as part of the Request for Proposal process, consider having the proposed providers on your “short list” demonstrate their system “live” for your institution at their site. Doing so allows you to potentially operate the system “hands on,” focusing on the following concerns and questions:

**General System Characteristics**

**GUI:** Do the applications in the system use a Graphical User Interface (GUI)?

**Appearance:** Do the applications in the system use a similar (i.e., appearance, use) user interface (again, GUI preferred)?

**New account setup:** (i.e., CIF look-up, features to prevent duplicate relationship setup, ease of use, integration to the core system, degree of manual effort required to supplement the data passed to the core system, speed of document preparation).

**Loan document preparation:** (i.e., CIF look-up, features to prevent duplicate loan relationship setup, features to tie direct and indirect borrowings, ease of use, integration to the core system, degree of manual effort required to supplement the data passed to the core system, speed of document preparation, inclusion of loan-pricing module).
**Information retrieval:** How easy or difficult is it to query the system? Are users able to include data from multiple applications (i.e., deposits of all types, loans, other) in the report?

**Customer reporting capabilities:** How are they prepared — by the users at the bank on-line (preferred) or does the bank have to request them from the vendor (not preferred)? Does the system allow gathering data from multiple applications (i.e., deposits of all types, loans, other) in reports?

**System Installation, Setup, and Training**

In addition to the demonstration of the existing system, the vendor should discuss in detail additional offerings or upgrades to the current system that are in development and when such offerings/upgrades will be available.

Will the vendor develop the network design, specifying the equipment (i.e, PCs, servers, LAN/WAN equipment, line speeds, etc.) required at the bank?

How many technical staff members will the vendor supply, on-site at the institution, to assist the institution staff during installation, and what will be their roles? Will these staff members be from the company or from a third party?

How much assistance can the institution expect in setting up the system for operations, (i.e., in setting system specifications, choosing operational parameters, codes and the like)?

How long does the vendor estimate setup (i.e., choosing parameters, setting specifications, other configurations, etc.) of the system will take?

How much time will be required to install equipment at the institution’s site?

How much training will the vendor supply, on-site at the institution and off-site at the vendor’s facilities?

**Customer Support**

What type of customer support is available (i.e., telephone, e-mail, fax, other) for technical and systems support (i.e., equipment, network and system)?

What type of customer support is available (i.e., telephone, e-mail, fax, other) for User support (such as a Help Desk)?

Do vendor personnel or third-party contract personnel deliver on-site support at the bank?

Would it be possible to review recent logs of user Help Desk questions, both system and user, to form an idea of the nature of user questions and evaluate response by the vendor?

Does the vendor have any customer satisfaction survey results that could be reviewed?

**Disaster Recovery**

Does the vendor have a disaster recovery plan?

Does the plan provide for restoration of communications with the financial institution as well as restoration of the data center?

If restoration of communications is not effective, does the vendor have recommended procedures for the financial institution to follow?
Is the financial institution allowed to test or participate in the testing of the disaster recovery planning (at least the portion that restores communications to the institution)?

**Client Reference Questionnaire**

Here are sample questions that you may want to consider asking when visiting client financial institutions that technology service providers have identified as references for their systems.

**Use of the System**

How long has the institution been using this system?

Does the system meet the requirements of the institution? If not, where does the system fall short?

How does this system compare with others that you have used, either at this institution or at others?

How many users do you have currently accessing the system? Are all users located in the institution or are they accessing the system remotely?

What general types of equipment are you currently using (i.e., workstation, network, communications), and are they adequate for your needs?

Have users found the system easy to learn and use? How much time and effort was required to train users on the system?

Does the Customer Information File (CIF) system function adequately?

Do you have difficulty with multiple-user relationships being established on the system; and if so, why?

Does the system require significant manual intervention, either to correct data input, particularly flags or options automatically set by the system, or to supplement information passed to the core systems (i.e., demand deposit and loan systems) from the platform systems (i.e., new accounts and loan document preparation systems)?

Do the reports that are automatically prepared by the system generally meet your needs; or have you been required to supplement the standard reports with other reports (i.e., PC generated)?

Do you find it easy or difficult to prepare custom reports on the system?

Have you requested customization of the system or changes to the system? If so, how were those requests received and handled?

**System Availability**

Is the system generally on-line and available for use when needed?

What is the general percentage of time that the system is online, in-service, and available during your normal business hours?

What is the general percentage of time that the system is online, in-service, and available after your normal business hours?

Are there any particular times when the system is unavailable. If so, why?
New Releases and Upgrades

How often has the system been upgraded with new releases?

Did the vendor provide you with sufficient notice of these new releases?

When the new releases were installed, did they work properly?

When the new releases were installed, did operations continue normally the following business day or were they disrupted due to problems with the releases?

Was the institution notified ahead of time when the vendor has made major equipment changes?

Did the installation or upgrade of equipment by the vendor disrupt your operations?

Customer Support

Is the vendor responsive to help or service requests?

What has been the typical response time for service or replacement of defective equipment?

What has been the typical time required to respond to user help-desk questions?

Do vendor employees or contract personnel come on-site to repair the system and/or equipment or respond to help requests?

Implementation and Conversion

How was the conversion experience?

Did the vendor provide a detailed conversion plan?

Did the vendor provide sufficient conversion management and adequately coordinate conversion activities to minimize disruption of the institution’s operations?

Did the vendor ensure that existing interfaces to other peripheral systems in use by the institution were maintained/provided for the new system?

Did the institution encounter any unexpected problems or costs during the conversion process?

Did the vendor provide sufficient post-conversion support?

General

Has the institution found the system to be cost effective?

Does the system allow the institution to be more efficient when compared to other systems they have used?

If the institution could make the decision over again, would it choose the same vendor/system?
Requests for Proposals

The end result of defining the various critical business needs of a system is the development of a Request for Proposal, or RFP. A request for proposal is a formal invitation to vendors to submit a proposal to the institution. In addition to specifying the various needs and requirements of a system, the RFP also provides critical background information about the institution and its processing environment, outlines the conditions that vendors must satisfy when submitting the proposal and provides information about how a winning vendor will be selected.

A well thought-out, carefully prepared RFP is the key to a successful evaluation of vendors and their respective systems by the Vendor Evaluation Team. By clearly defining the requirements that the system must meet and setting a standard format for vendors to follow as they prepare the proposal, the RFP provides a method for objectively comparing competing proposals and narrowing the institution's focus on prospective systems.

Key Elements of a Successful RFP

Confidentiality and Non-Disclosure Statement. The institution should state clearly that it is providing information to the vendor regarding its strategic plans, operations, services, and in some cases, customers. This information is only provided to the vendor for the purpose of submitting a specific proposal, and should not be disclosed in any form to third-parties without the written permission of the institution.

Scope, Purpose and Objectives. This section should clearly spell out for the vendor what the institution intends to accomplish through its request for a proposal. For example, the purpose of the RFP is to define for the vendor the current and anticipated processing needs of the institution in a particular area. The objectives are to have the vendor propose specific solutions to meeting those needs. Applications covered by the RFP should be clearly defined in this section. For example, it should indicate that the institution is seeking a document imaging solution, or that the institution is seeking a core processing system solution and whether it will consider outsourced solutions, in-house solutions or both.

Response Instructions. Instructions specifying the format, timing and other general requirements of the vendor's response should be provided. These requirements might include the number of responses required and whether the response should be presented in electronic or paper format. Specific information requirements of the vendor should be detailed and might include such information as:

- History of the vendor's organization.
- Number of installed users, number of new users in the past year, and the number of users terminating service in the past year.
- Organizational structure.
- Location and responsibilities of all organizational units involved in servicing the institution's relationship with the vendor.
- Audited financial statements.
- Strategic plans and growth projections.
- Business contingency plans.
- Results of customer satisfaction surveys or evaluations of third parties.

Proposal Evaluation Criteria. Factors that the institution will use to evaluate the competing proposals should be clearly defined for each vendor. Such factors might include the:
Vendor’s performance record in meeting the requirements of its current customers.

Vendor’s financial stability, longevity, and strength.

Vendor’s commitment to remaining a provider of or processor of the proposed system.

Costs of implementing the solution, including acquisition, conversion and on-going costs.

Degree to which the proposed system meets the institution’s critical business needs.

Ability of the proposed system to interface with existing peripheral systems used by the institution.

Adequacy of controls and security in the proposed system.

**Background and History.** To help the vendor understand the unique aspects of the institution’s business and operations, information should be provided concerning the institution’s history, general nature of the institution’s business, general profiles of its customer base and current processing environment. Future business plans, including growth projections and new product and service offerings that might influence a vendor’s proposal should also be included.

**Products and Services.** Specific information should be provided about the institution’s products and services. If the RFP seeks a proposal for a new core processing, expansive information should be provided about product and service features, as well as account and transaction volumes. It is also helpful to include product and service brochures as appendices to the RFP.

**Current Processing and Data Communications Environment.** The vendor will need to know the type of platform, including mainframe computers, servers and network devices and lines, on which the institution currently operates. This is particularly important if it is the institution’s intention to maintain and operate the new system in this environment. A schedule of computer hardware that will be used in processing, or with which the system will be required to interface, should be provided.

Additionally, the vendor will need to know what other systems, applications and software the new system will be required to operate and interface. A complete inventory of such systems and applications, including release versions, should be included in this section of the RFP. The institution should also indicate to the vendor whether it will consider replacing any of these systems and applications, or if the new system must interface with them.

**Critical Business Needs.** Using the specific information developed by institution employees, the specific system capabilities and requirements of the institution should be defined. The institution may want to organize the information in this section by application type, product, or business function. Regardless of the manner chosen, there are certain general and specific information that should be obtained. General requirements might include:

- Conversion support provided by the vendor.
- Training provided by the vendor.
- Software customization, specific to the institution, permitted by the vendor.
- Level of telephone and on-going support provided by the vendor.

**Specific requirements might include:**

- Ability to operate in a particular equipment and communication environment. Critical application features, such as interest calculation methods, fee calculation methods, etc.
Other application features, such as ability to produce required tax statements, ability to allocate income and expenses, ability to process specific product types, etc.

Ability to interface with specific peripheral systems

**Contract Requirements.** This section of the RFP should solicit information regarding the vendor’s contract provisions and to communicate specific contract requirements of the institution. Issues covered include:

- Term of the contract.
- Commitment from vendor to maintain the software in compliance with banking and accounting regulations.
- Commitment to provide regulatory updates in a timely manner.
- Costs of upgrades.
- Penalties and time frames associated with early termination of the contract.
- Performance guarantees and performance measures.
- Remedies available to the institution if performance does not meet guarantees.
- Price guarantees, including de-conversion costs.
- A commitment on the maximum amounts of maintenance increases each year.
- Customary payment terms.

**References.** The vendor should provide the institution with a list of users that can be contacted and visited to evaluate the performance of the vendor and the proposed system. The institution may also want to request a list of new users, and those users who terminated service or replaced the vendor’s system in the past year.

**Service Level Agreements**

Many financial institutions have turned to service level agreements as an effective tool for measuring and monitoring service provider performance. Service Level Agreements (SLAs) are contractually binding clauses documenting the performance standard and service quality agreed to by the bank and service provider. Consider using SLAs to specify precisely the performance standard the institution expects to receive from the service provider.

As outlined in a recent FDIC technical bulletin, the SLA’s primary purpose is to specify and clarify performance expectations, as well as establish accountability. A well-designed SLA will recognize and reward, or at least acknowledge, good service. It will also provide the measurement structure — or performance metric — to identify substandard service and trigger correction or cancellation provisions as warranted. In today’s outsourcing environment, incentives or penalties in the SLA can be an effective tool for managing service. If services received do not measure up to expectations, direct consequences, such as reduced levels of compensation or a credit on future services, would result.

The FDIC has put together the following helpful outline for a service level agreement for illustration purposes. While not to be relied upon as a model contract for any specific service agreement, it can nonetheless guide you and your institution’s counsel in the formation of an SLA that meets your specific needs.
Sample Service Level Agreement Structure

Purpose:

This agreement is between Buyer and Vendor. This document outlines the service level roles, responsibilities, and objectives of Buyer and Vendor in support of the given functional area.

Scope of Services:

Vendor will house, manage, and operate all hardware and software necessary to provide Internet banking applications to Buyer.

Service Category:

This SLA addresses application availability.

Acceptable Range of Service Quality:

The Internet banking application shall be available at least 99.5% of each week.

Definition of What is Being Measured:

“Availability” will be measured as the percentage of minutes each day that the Internet banking application will be able to receive and respond to messages from the Internet. The server’s ability to receive messages will be ascertained using time-check availability software.

Formula for Calculating the Measurement:

System availability shall be measured as the number of minutes per day that the Buyer’s Internet banking application is capable of receiving and responding to messages from the Internet divided by 1,440 (the total number of minutes in a day).

A 30-minute period from 2:00 AM to 2:30 AM shall be excluded from the calculation because Vendor will be performing system maintenance at this time each day.

Relevant Credits/Penalties for Achieving/Failing Performance Targets:

If Vendor is unable to provide this service level to Buyer, Vendor will provide priority support to Buyer until performance levels are met. Service below the prescribed level will result in a rebate of 50% of the monthly fee for the month in which the exception takes place.

If Vendor fails to provide the agreed upon service level for more than two consecutive months, Buyer shall have the right to renegotiate the contract and/or terminate this agreement.

Frequency and Interval of Measurement:

The system’s availability shall be measured daily by Vendor using the time-check availability software. Vendor shall submit monitoring reports generated by this program to Buyer on a weekly basis.

Buyer’s Responsibilities:

Buyer shall review all monitoring reports and advise Vendor of any deviations from this agreement in a timely manner. (Include any other items that Buyer will need to do so that Vendor may perform its tasks.)
Vendor’s Responsibilities:

Vendor shall assume responsibility for customer communications from the point that customer messages leave the Internet service provider.

Vendor shall ensure that all messages are processed in a timely fashion. (Be sure to define the specifics of “timely” standards.)

Vendor shall ensure that the system shall be able to accept and respond to 1,200 inquiries per minute. (Include any other items that Vendor will need to do to provide the prescribed level of service to Buyer.)

Escalation Guidelines:

In the event that Vendor is unable to meet the terms of this agreement, the CIO of Buyer and IT Manager of Vendor shall discuss resolution of the situation. If Vendor will be unable to provide service for more than two hours, Vendor’s contingency operating plan shall be invoked.

Renegotiations:

Authorized representatives of Buyer and Vendor must mutually agree upon changes to this SLA.

All changes must be made and agreed to in writing. Either party may request review of this SLA at any time. Each party will review the SLA annually and advise the other party of any desired changes.

Annual Reviews of Service Providers

Having your institution and your business units annually review the performance and status of each of your institution’s service provider arrangements helps you ensure that each of these arrangements is properly monitored. This form is designed to assist you in determining how well your front-line management is overseeing their providers, as well as if there have been any changes in that status of any provider over the course of the year. Any significant changes in a provider that has been deemed to have a high level of risk to customer information, based on your risk assessment, should be brought to the attention of the board or the board committee responsible for oversight of the institution’s customer information security program.

Service Provider Survey

Name of Service Provider:

Date Initial Contract Signed:

Location of Signed Contract:

Employee Responsible for the Ongoing Monitoring of the Provider and the Contract:

(name, phone and location)

1. What is the title of your line of business?

2. What business function is provided by the service provider? Briefly describe the services provided:

3. Does your line of business own this outsourcing arrangement?

   a. If not, then which legal entity or line of business does?
   b. If you depend on this outsourcing that you do not own/control, is there a feedback process for poor service?

4. Do any other of our institution’s business units use or receive services from this provider covered under
this contract? If yes, please specify:

5. Have there been any changes in the nature of the services provided over the last 12 months? If yes, please describe:

6. Identify how the terms of the contract are being monitored and by whom:
   a. How do you identify and measure performance issues?
   b. Is there a Service Level Agreement in the contract that establishes standards for quality and performance levels?

7. Does the contract have set (periodic) renewals, or does it continue until one party invokes a termination clause?

8. Describe any performance issues arising during the prior 12 months, including means of detection and resolution.
   Are there any performance issues still outstanding?

9. Does the service provider have adequate business contingency plans?
   How do you verify this?

10. Does the service provider company have adequate information security procedures?
    How do you verify this?

11. Has either a credit analysis or some other means of assessing the financial condition of the service provider been performed during the prior 12 months?
    By whom?

12. Is the service provider’s financial condition satisfactory?
    Are there any concerns?

13. Does the arrangement involve sharing customer information with the service provider?
    If “yes,” for corporate customers, or for retail customers, or for both?

14. Overall, are you satisfied that services provided are of acceptable quality, and that the service provider’s internal controls and financial condition are adequate to protect our institution?

Name: 

person completing review

Signature: 

Date: Phone:
Name: line of business senior executive

Signature:

Date:  Phone:
Both the physical and cyber aspects of business continuity and recovery must be addressed in order for your institution to properly safeguard customer information. And in today's world, the two really cannot be separated.

Planning for business continuity and recovery have three aspects: prevention, anticipation, and mitigation. The purpose of planning is thus to avoid and minimize interruptions in business continuity, identify events that will disrupt your operations and related consequences, and take steps to manage these events to minimize their impact when they do occur. The tools in this section cover both the physical and cyber aspects of business continuity. Many of the other tools contained in this toolbox also relate to business continuity and recovery. For instance, the risk assessment process discussed in Tool 2 has a direct relationship to business continuity, as an important step toward prevention.

**Structuring Your Business Continuity Plan**

This document provides a structure for your institution to consider when revisiting your business continuity and recovery plan. Business continuity planning and execution occurs in four phases:

**Operational Phases**

1. **Normal Operations Phase** - The period before an event occurs. Consider:
   1. Defining the areas of exposure
   2. Educating staff
   3. Performing business impact analysis
   4. Involving key people in developing strategies
   5. Developing the plan(s)
   6. Taking preventive measures
   7. Identifying and assigning routine actions to facilitate responding to actual contingencies
   8. Testing and maintaining the plan(s)
   9. Promoting business continuity planning awareness and preparedness

2. **Emergency Response Phase** - The first few hours immediately following an event, where the extent of the problem is identified and an organized response is mustered.

3. **Alternate Procedures Phase** - The time after the emergency response, when interim procedures are used to support essential business functions until normal processing capabilities are restored.

4. **Restoration Phase** - The time period given to restoring a processing capability to its normal condition. (This period is expected to overlap with the Alternate Procedures Phase.)
Business Continuity Planning

Based on your risk assessment, your institution should consider developing business continuity plans for core business processes, key business partners, critical external infrastructure services, and perhaps certain critical inventoried hardware, software or embedded systems. The risk assessment demonstrated which systems and applications are more critical than others. The risk ranking becomes important, because as areas requiring business continuity plans are identified, constraints relating to costs, resources and time will surface. Those most necessary to the continued functioning of the institution must be done first. Executive management must agree to and support the ranking and allocate funds and staff for the development of the business continuity plan.

The business continuity plan should address:

- To whom does the plan need to be communicated
- Under what conditions (triggers) will the plan be invoked
- How long the loss can be endured before implementing the business continuity
- Who has the authority to invoke the plan
- Who has the responsibility for invoking the plan
- Who should have copies of the plan
- Who has the original and what is the date of the most current plan
- How frequently should the plan be updated
- The level of service to be provided during the "outage"

Business Continuity Plan Formats

Consider putting business continuity plans in place and satisfactorily tested to perform the following procedures, corresponding to the four phases identified above.

1. Normal Operations Procedures

This section should outline tasks and responsibilities necessary to support and maintain an effective ongoing business continuity and recovery plan before an event occurs. Examples of such tasks include file backup procedures/policies, inventorying and maintaining supplies, forms, and materials required for alternate procedures, periodic business continuity plan testing, etc.

2. Emergency Response Procedures

Emergency response occurs during the first few hours immediately following an event. This section of the plan identifies activities that may need attention during this time. It is intended to ensure an organized response and to provide a checklist so that important decision-makers and issues are not inadvertently overlooked in the confusion that can accompany the event. It should contain actions assigned to specific individuals and/or an Emergency Response Team.

3. Alternate Procedures

It is important that comprehensive and detailed work-around plans be developed, documented, tested and placed on several library shelves in anticipation of the day they will be needed. For these work-around plans,
the institution's personnel will want to make sure they understand what processes will need to be performed manually or without computerized support. It will also be important to acquire specialized supplies, forms or equipment in advance. It would be wise to conduct a dry run to ensure that all the processes will work, in the event of an emergency. This should also highlight any training needs. It is not necessary that the work-around be as robust and complete as the "real thing." The purpose of the dry run is for your institution to make sure you are capturing all the essential aspects of your processes, have a way to continue to do business, and have a way to "recover" from the temporary disruption when the applications "come back on line."

Employees who are directly responsible for applicable business functions should develop your alternate procedures. These procedures should address 3 sub-phases:

A. **Start-up.** This section of the plan identifies specific preparations needed to make a transition from normal business procedures to an alternate processing mode.

B. **Support of essential business functions.** This section describes how people in applicable functional areas of the institution have agreed to support vital business functions until normal operations can be restored.

C. **Data recovery.** In this section, the plan covers functional area responsibilities for retaining transactional, process or other data (that occurred during the alternate procedure period) so that files and databases can be updated when normal processing capability is restored.

Developing alternate procedures involves the preparation and partial implementation of alternative work processes in the event of a business failure of varying proportions. It was perhaps the most difficult aspect of solving the Year 2000 problem, because it involved a disciplined investigation into all aspects of a corporation's business to locate those points where significant risk can occur which could immobilize a business's viability.

Invite users, experts and support personnel. An alternate procedure must be broad based and have wide business support. Because it can involve the suspension/elimination of some existing processes, those areas of the business which are potentially affected need to be involved in the decision process. The user organization knows the potential impact of doing without certain key business processes, and know what they can live with and without in an emergency situation. The duration of the emergency will affect the business continuity chosen. An outage of an hour or two will be handled differently from an outage of two weeks or more, consequently, business continuity alternatives relative to the duration must be developed. Representatives from infrastructure areas, such as facilities, security, food service, etc., should also provide input.

4. **Restoration Procedures**

Restoration involves the steps necessary to return to a normal business function. This section includes addressing the duties and responsibilities of individuals to actually get the hardware, software, or embedded system malfunction corrected. It should also include the procedural steps to transition from operating under an alternate procedure at reduced efficiency to normal operations and efficiency.

**Disaster Recovery Planning – An Overview**

The following is adapted from Security Education System's Disaster Recovery Manual and should prove helpful for revising your institution's disaster recovery plans.

**Overview**

A disaster is any event that will significantly - and negatively - affect the institution's operations. Examples of "traditional" disasters include fires, floods, hurricanes and earthquakes. Examples of "non-traditional" disasters include terrorist strikes, toxic waste dispersions, computer system crashes and labor strikes.
Losses caused by a disaster are often disproportionately costly in relationship to the size and complexity of the actual event - and many of the losses are preventable. Disasters actually result from three types or combinations of incidents, caused by:

- Natural or cataclysmic events (e.g., earthquakes, fires, floods and storms); Human behavior (e.g., robberies, bomb threats, acts of arson, hostage events or transportation strikes); and
- Technological breakdowns (e.g., power outages, computer crashes and virus attacks).

**What Should A Disaster Recovery & Business Resumption Plan Do?**

Recovery and resumption is actually a two-part exercise:

- "Disaster recovery" is the process of restoring the entire institution's ability to operate; and
- "Business resumption" is the process of re-opening each of the institution's components – and testing and revising the process based upon the results.

So what is disaster recovery planning supposed to do for the institution? It's all about:

- Making do with whatever's left;
- Buying time to:
  - Recover from the initial impact;
  - Restore basic operations;
  - Resume normal operations; and
  - Replace damaged equipment & facilities; and
  - Redundancy -- a duplication of critical people, places and things.

**What is Your Disaster Recovery & Business Resumption Plan supposed to do for the community?**

It's all about:

- Stability - ensuring the survival and livelihood of at least its own personnel;
- Appearance - remaining a visible and integral part of the community's infrastructure; and
- Cash flow - using the institution's operations and resources to:
  - Store, transport and disburse cash;
  - Negotiate payable instruments; and
  - Accept deposits.

Usual security and operations policy and procedures are simply not enough to adequately protect your personnel, customers and other persons, facilities, assets and records from disasters - and the predictable aftermath. Targeted techniques that work well for natural or cataclysmic, human-caused and technological disasters are necessary to create a consistently safe and secure working environment within the entire institution -- and to close the "windows of opportunity" to losses often caused by:

- Mistakes;
National events occurring daily demonstrate that it is not a matter of if - but when - a disaster will significantly affect your institution's operations. This will naturally cause an interruption of customer services. And your customers will need your services during a disaster. If a natural, technological or human-caused disaster strikes your institution - are you now prepared to successfully:

- Insure the continuity of organizational leadership and the effective management of all personnel, functions, facilities, assets and records?
- Notify your employees of new work locations, telephone numbers and critical persons to contact - and of changes in the organization's leadership structure, duties and responsibilities and safety concerns?
- Notify your customers of new business locations, telephone numbers, critical persons to contact and the evolving customer service changes?
- Notify your vendors and service providers of new delivery schedules and locations, critical persons to contact and order new equipment and supplies?
- Recover your critical hard-copy documents, such as contracts, charters, licenses, accounting records and other printed business records?
- Recover your computerized data files, such as accounting and inventory programs, personnel, member and vendor databases and word processing files - such as form letters, marketing and advertising information and general correspondence?

No one is exempt from a disaster, and most people are unprepared if a disaster erupts. We should prepare as if the disaster will exceed our ability to respond effectively. In other words, prepare for a "worst-case" scenario.

**What Are The Best-Recognized Types Of Disasters?**

A disaster may also result from a sudden, unexpected occurrence that poses a significant threat to the institution's personnel, customers, facilities, assets, records, or its delivery of services. These events are categorized as:

- Localized (e.g., likely to affect only the institution);
- Community based (e.g., likely to affect an expanded area contained within a three-mile radius from the disaster epicenter);
- Regional based (e.g., likely to affect several adjoining cities and counties); and
- Statewide based (e.g., likely to affect the state and adjoining states).

**What Are The Most Commonly Reported Disasters?**

The most common - and preventable - disasters for which insurers pay often unnecessary claims each year are caused by:

- Fires;
Water leaks;  
Power outages;  
Virus attacks;  
Premises liability issues; and  
Human errors.

What Will Likely Happen During A Disaster?

The key to recovering successfully from a disaster is to have a plan in place before the disaster strikes - a set of simple, effective guidelines and procedures for all people to follow. Just as a ship without a rudder is at the mercy of the tides, an institution without a plan is at the mercy of events.

Human beings often make inappropriate decisions during a crisis. If we have a plan for coping with most emergencies already prepared and shared with others, we stand a better chance of surviving any emergency and recovering rapidly.

A contingency plan helps an institution respond to a regional disaster that follows this logic:

- It is not a matter of if - but when - a disaster will occur;
- The effects of a disaster will likely exceed the community's and the institution's response capabilities;
- The evolution of events following a disaster will be predictable and cyclic;
- The community and the institution will likely be without outside help - including emergency services agencies, vendors and service providers - for a period of time, including:
  - Basic emergency and transportation services, such as police, fire and medical assistance, and both public and private forms of transportation. Routine calls for service may not be answered - and the agencies' priorities will likely involve life-threatening or life-saving situations only;
  - Food and survival supplies: Deliveries to food stores and hospitals may be interrupted or hijacked - and citizens will immediately strip stores of existing supplies of all kinds, while stockpiling their own reserves;
  - Water supplies and sanitation: Water and sewer pipes may break, crack or clog - reducing or eliminating water flow;
  - Electrical power: Power lines may be destroyed, overloaded or collapse - causing every electrically-dependent device to become unusable;
  - Products and services delivered by vendors and service providers: The geographical area affected by the disaster may be closed to outside traffic - or the vendors will be too busy answering calls for service from other clients who have also been affected by the disaster;
  - Telecommunications services: Telephone trunks and switching stations will become overloaded by people trying to call into or out of the affected area; and
Transportation services: Freeways, highways and surface streets will become gridlocked by people trying to get into or out of the affected area.

- The greatest losses will occur because of the community's and the institution's inability to react to the disaster - appropriately and immediately;
- The governor of the state or another competent authority will declare the community a disaster area;
- Martial law will be declared, the National Guard will be activated and basic civil rights will be suspended;
- Traditional roles and routine activities within the community will be temporarily suspended, causing the reassignment of personnel to fulfill necessary roles and functions, with temporary powers, duties and responsibilities;
- The institution will not be able to recover or restore all functions at the same time;
- Only 35% of the institution's staff will likely be available during the first three (3) days following the disaster:
  - Critical people (including the board of directors) will likely be unavailable;
  - Critical places will likely be uninhabitable;
  - Critical things will likely be unusable; and
  - Employees who are proficient in normal times will likely exceed performance expectations during emergencies.

**What Should Be the Goals of the Disaster Recovery & Business Resumption Plan?**

The three primary goals of disaster recovery and business resumption planning are to:

- Eliminate or reduce the potential for injuries or the loss of human life, damage to facilities, and loss of assets and records. This requires a comprehensive assessment of each department within the institution, to insure that appropriate steps have been taken to:
  - Minimize disruptions of services to the institution and its customers;
  - Minimize financial loss;
  - Provide for a timely resumption of operations in case of a disaster; and
  - Reduce or limit exposure to potential liability claims filed against the institution, and its directors, officers and other personnel.

- Immediately invoke the emergency provisions of Disaster Recovery & Business Resumption Plan to stabilize the effects of the disaster, allowing for appropriate assessment and the beginning of recovery efforts. We then minimize the effects of the disaster and provide for the fastest possible recovery.

- Implement the procedures contained in your disaster recovery and business resumption plan according to the type and impact of the disaster. When we implement these procedures, we must prioritize all recovery efforts as follows:
• Employees: Not only must we help to ensure their survival as a basic human concern, but because of their anticipated performance in helping other persons on the institution's premises when the disaster strikes;

• Customers: As we do with employees, we must help to ensure the survival of or care for customers affected by the disaster: physically, mentally, emotionally and financially;

• Facilities: After ensuring the safety of employees and customers, we then secure each facility as shelter for both people and assets;

• Assets: Conducting a damage assessment will determine which assets have been destroyed, which ones are at risk and what resources that we have left; and

• Records: Documenting the disaster and the actions taken by the institution's personnel - when combined with comprehensive videotapes of facilities that are obtained during routine facility inspections - reduce the likelihood of legal actions while helping to assess the responsibility for losses.

What Issues Should The Disaster Recovery and Business Resumption Plan Address?

To be effective and to remain in compliance with regulations, your institution's disaster recovery & business resumption plan should contain at least:

✓ The institution's philosophy, mission statement and goals regarding disaster recovery and business resumption;

✓ Written and approved executive succession instructions;

✓ The appointment of a temporary Disaster Management Executive Committee for the term of the emergency that is empowered to act in the absence of the institution's Board of Directors;

✓ Clearly defined guidelines and scope of all disaster recovery and business resumption efforts, based upon a thorough risk-assessment;

✓ Clearly defined duties, authorities and responsibilities for each employee classification, with designated primary and alternate department leaders and staff personnel to manage critical functions;

✓ A business recovery plan for each branch, department, facility and function within the institution - and for essential service providers;

✓ Designated and equipped sites for assembling personnel and for housing specific operations;

✓ A well-documented testing and evaluation process conducted at specified intervals - and at least annually;

✓ A comprehensive training program for all personnel at all facilities, conducted at specified intervals - at least annually - that may also include the:

  • Identification and operation of utility shut-off devices;

  • Location of emergency staging areas;

  • Basic first aid and survival techniques; and
- Emergency responsibilities and re-assignment plans for all positions.

✅ Written copies of the final Disaster Recovery & Business Resumption Plan distributed to branch and department leaders -- including a complete list of appropriate emergency response agencies and facilities.

**How Should the Disaster Management Team be Created?**

The members of the institution's Disaster Management Team are drawn from the institution's available personnel resources - and they may also be board members, vendors and service providers. The Disaster Management Team functions as a strategic planning and tactical response unit. Team members are often assigned temporary duties, responsibilities and levels of authority beyond their normal employment classification.

The Disaster Management Team usually contains the executives, managers and department heads that have functional responsibilities involving branches, departments or facilities. There is no one "right" way to develop and implement a plan - nor to assign emergency responsibilities. The variables will be affected by the:

✅ Type and asset size of the institution;

✅ Number and qualifications of personnel;

✅ Number and configuration of facilities; and

✅ Thoroughness of the risk assessment.

Condensing and streamlining business operations during a disaster is critical to getting the institution "back up and running" - quickly and smoothly. This also means using the fewest personnel to accomplish the greatest amount of tasks. A suggested format for assigning responsibilities includes:

✅ The Disaster Management Executive Committee, which is the temporary legal body that's responsible for creating and implementing a comprehensive Disaster Recovery & Business Resumption Plan for the entire institution, in the absence of the Board of Directors. The Committee usually consists of the institution's President/CEO, selected executives and senior managers - and it may also contain members of the institution's Board of Directors.

✅ The Disaster Management Team Chairpersons, who are responsible for assigning the research, development and implementation of the Disaster Recovery & Business Resumption Plan throughout the institution. The Chairpersons are also responsible for assuming control over business operations during and after the disaster, until business operations return to normal. The Chairpersons are responsible for providing effective leadership and administration of the institution's recovery efforts - and for making decisions and giving directions.

✅ The Disaster Management Team Coordinators, who are responsible for creating a comprehensive Disaster Recovery & Business Resumption Plan for the institution - and for following the directions and implementing the decisions made by the Chairpersons and the Disaster Management Executive Committee during a disaster. The Coordinators are responsible for providing effecting management and implementation of the institution's recovery efforts - and for monitoring and adjusting the process flow.

✅ The Disaster Management Team Department/Branch Leaders, who are responsible for acting as Coordinators for their respective areas of responsibility - and they report directly to the Disaster Management Team Coordinators, and
Service providers, vendors, insurance representatives and legal counsels, who are responsible for providing guidance and advice regarding their particular areas of expertise - and they report directly to the Disaster Management Team Coordinators.

Summary

It's common to underestimate the importance of having a plan. It's also a common - and mistaken - belief that the effectiveness of such a plan should be judged by the number of pages it contains or its weight. The only true means to gauge a plan's effectiveness is: "Did it work?"

Ill-conceived beliefs and overlooked issues often cause a project to fail. As you prepare to develop and implement a Disaster Recovery & Business Resumption Plan - or reassess an existing one - consider using these simple guidelines to enhance your success:

- Get the board's full and complete support to do whatever it takes to put the plan in place - and update and train board members periodically;
- Place your best leaders in charge of administration - regardless of the positions that they normally hold - and train them;
- Place your best managers and supervisors in charge of operations - regardless of the positions that they normally hold - and train them;
- Involve your best employees in the development and implementation process -- and train them about the decision-making process and their respective roles;
- Hold everyone personally responsible for results;
- Keep the plan simple and logical and use it as a bullet-point guide for experienced personnel to use - it's not supposed to be an operations manual;
- Flow-chart every business process so that any manager can re-install any function;
- Make certain that the risk assessment process includes a thorough analysis of those issues that are most likely to be affected by a disaster, including:
  - Telecommunications (e.g., voice, fax, modem and cellular);
  - Transportation (e.g., highways, rental vehicles and public transportation);
  - Essential services (e.g., government, medical and child care);
  - Essential supplies (e.g., food, money and fuel); and
  - Document the entire planning and implementation process, particularly tests.

Service Provider Business Continuity Questionnaire

The Business Continuity Service Provider (SP) Survey, developed by RISConsulting LLC, can establish a baseline of service provider continuity program information for your institution, and help in gathering details to ensure that your service providers can be accurately evaluated as to their potential risk to your institution.

The survey questions address general information regarding a service provider’s business continuity program, recovery, data backup, service interruption, and testing.
1. Business Continuity Program
Do you have a business continuity program in place?

- [ ] Yes
- [ ] No

Describe:

Have you conducted a Business Impact Analysis (BIA)?

- [ ] Yes
- [ ] No

Describe:

Do you have contingency plans that address outages that may affect customers?

- [ ] Yes
- [ ] No

Describe:

Do you have recovery plans that address technology-reliant customers?

- [ ] Yes
- [ ] No

Describe:

Have you prioritized the recovery of your critical business functions?

- [ ] Yes
- [ ] No

Describe:

Have you prioritized recovery of critical technology?

- [ ] Yes
- [ ] No

Describe:
2. Recovery
What is your Recovery Point Objective (RPO) for customers? (The point in time where you data is recovered and synchronized.)

(8 hrs, 24 hrs, 48 hrs, etc.) Note here:

What is your Recovery Time Objective (RTO) for customers?

(8 hrs, 24 hrs, 48 hrs, etc.) Note here:

Do you have procedures for incident reporting?

Do you have incident escalation procedures?

3. Data Backup
Do you backup your critical data?

○ Yes  ○ No

Describe: (Manually, Automatic, both)

Where do you backup your critical data?

Local Hardrive: ○ Yes  ○ No
Onsite portable storage media: ○ Yes  ○ No
Redundant server at the same site: ○ Yes  ○ No
SAN (Storage Area Network): ○ Yes  ○ No
Offsite on portable storage media: ○ Yes  ○ No
Redundant server at a different site: ○ Yes  ○ No
Shared Drive: ○ Yes  ○ No
__Other  __I don’t know

Do you rely on: (If yes, how long could you function effectively without access? Specify: Less than 2 hrs, 2-24 hrs, 1-3 days, 4-7 days, More than 7 days)

Mainframe: ○ ..  ○ ..
Servers: ○ Yes  ○ No
Workstation-based applications: ○ Yes  ○ No
Applications stored on a shared drive: ○ Yes  ○ No
Intra/Internet: ○ Yes  ○ No
Intra/Internet:  
- Yes  
- No

Email:  
- Yes  
- No

__Other ___ I don’t know

Do you maintain critical data for your customers?

- Yes  
- No

Do you store customer data? If so, please specify for how long.

- Yes  
- No

Do you have the ability to perform restore procedures upon customers request?

- Yes  
- No

Do you have documented procedures in place to hold, accept or deliver work if your customers are affected by an outage? If so, please describe in brief.

- Yes  
- No

Does your transmission of electronic data have failover capabilities? If yes, please explain.

- Yes  
- No

Do you have redundant hardware to support manual or automated failover?

- Yes  
- No

If you have failover technology, please specify where it resides.

___ At Same Location ___ Geographically separated

Other please describe:

4. Service Interruption

What is the maximum amount of time before your customers(s) would be affected by an interruption in your service?

- Immediate  
- 2-4 hours  
- 4-8 hours  
- 8-12 hours  
- 12-24 hours  
- 24-36 hours  
- 36-48 hours  
- 48-72 hours  
- 72-96 hours  
- 5 days +

Do you have documented workarounds in case of a systems (network or application) or telecommunications (i.e. phone, fax, e-mail, etc) failure?
5. Records Management
Do you have any processes without written documentation, or that only one individual is able to perform?

Yes  No

Please Describe:
Where are your original paper records stored?
Please Describe:

Do you have records for which only the original exists?

Yes  No

6. Testing
Have you?

Tested Recovery Time Objectives (RTOs):  Yes  No  NA
Tested business resumption plans:  Yes  No  NA
Tested technology recovery plans:  Yes  No  NA
Conducted recovery tests with customers:  Yes  No  NA
Tested your production environment:  Yes  No  NA

Re-addressed your network at your recovery site for a test or actual recovery:

Yes  No  NA

Used a simulated production or test environment for recovery testing:

Yes  No  NA  I don't know

Other:

Do you have an active test environment?

Yes  No
Are you planning on testing any services that you provide to customers this year?

☐ Yes  ☐ No

Can we have an observer on site when you test?

☐ Yes  ☐ No

Can we coordinate a test with you?

☐ Yes  ☐ No

How much lead-time would you require for coordinating a recovery test?

Describe:

Who are the appropriate contacts in your organization for recovery testing?

Please note:

When was your last test?

Please specify quarter/year:

7. Miscellaneous

Does state or federal law regulate any of your business processes?

☐ Yes  ☐ No

Describe:

Has your continuity program been audited? If so, please specify date and type of audit (SEC, OTS, etc.)

☐ Yes  ☐ No

Describe:

8. Additional remarks:

Please provide the following information, if possible, along with your completed survey.

- A copy of your business continuity plan(s)
- A copy of your incident escalation procedures
- A copy of your test schedule
- A copy of your recent test results

Thank you for your participation!!
Tool 6: Training Your Employees

Employee training is a key component of any security program. All employees and officers must understand the importance of protecting the confidentiality and security of customer information, and be familiar with the procedures they are expected to follow when accessing, handling and storing customers’ personal information. Senior management support is critical to any training effort. Your employees will appreciate your efforts to improve customer privacy protection and bank security.

Safeguarding customer information in your institution is everyone’s business, from the backroom to the boardroom. Having your employees understand their obligations for securing information means giving them the tools to do so. One of the most important areas of employee training with regard to customer privacy is how to recognize and deal with pretext calls. This section draws from the ABA’s Financial Privacy Toolbox preventing pretext calling tools to assist your employees in spotting and preventing such calls.

Training Your Employees

Employee training is a key component of any security program. All employees and officers must understand the importance of protecting the confidentiality and security of customer information, and be familiar with the procedures they are expected to follow when accessing, handling and storing customers’ personal information. Senior management support is critical to any training effort. Your employees will appreciate your efforts to improve customer privacy protection and bank security.

It should also be clear to all employees that significant disciplinary actions will be taken against anyone violating the institution’s privacy or information security procedures. It is particularly important that supervisors appreciate the importance of limiting access to customer records and the problems caused by failures to maintain that protection, as they must assume the responsibility for implementing disciplinary measures.

In their regulations implementing the Gramm-Leach-Bliley Act’s Standards for Safeguarding Customer Information, the regulatory agencies included a guideline that institutions should include as part of their security program a “training component designed to teach employees to recognize and respond to fraudulent attempts to obtain customer information and, where appropriate, to report any attempts to regulatory and law enforcement agencies.”

One of the most important areas of employee training with regard to customer privacy is how to recognize and deal with pretext calls. This Tool includes a training manual that will help your staff effectively cope with pretext calling situations. ABA has also prepared an Identity Theft Communications Kit (sent in July to all ABA member banks) to help you be proactive in your community by teaching your customers how to protect themselves from identity theft.

Training Guide For Senior Management

- Discuss the history of protecting the confidentiality of information and how vital it is to protect customer trust.
- Discuss customers’ sensitivity to financial (and medical) privacy (see Tool 6).
- Distribute the Privacy Awareness Tips for Employees (in this tool), and show ABA’s Consumer Privacy Training Video.
- Review your code of ethics on use and protection of customer information (see the Sample Code Of Conduct provided in Tool 1).
- Review the disciplinary measures for violating policies and procedures.
- Go through your privacy policy statement in detail.
- Review any additional responsibilities and lines of authority (such as new duties of a privacy manager or expanded authorities of the security officer).
- Review the benefits of information sharing within your institution and ask employees for examples of benefits that they see in their jobs.
(See Customer Benefits of Information Sharing in Tool 6.)

Practice answering customer questions on privacy (use the Frequently Asked Questions document in Tool 6 to help you with this).

Also look at ABA’s Financial Privacy Communications Kit and the Identity Theft Communications Kit.
Information Security in the Workplace: What Every User Should Know

By
Melissa J. Dark, Ph.D., Assistant Professor & Continuing Education Director
Information Security in the Workplace: What Every User Should Know ©

Published by: CERIAS, The Center for Education and Research in Information Assurance and Security, Purdue University, West Lafayette, Indiana.

Text and art copyright © 2000 by CERIAS, The Center for Education and Research in Information Assurance and Security, Purdue University, West Lafayette, Indiana. All rights reserved. No part of this manual may be reproduced or transmitted in any form, by any means without the prior written consent of the publisher.
Table of Contents

Introduction 3

Section 1: The Value of Information and Information Security 4

Section 2: Protecting the Organization’s Assets 7

Section 3: Security Risks and Countermeasures 11

A. Password Basics 12
   Why Worry About Passwords? 12
   Password Protection Fundamentals 13

B. Physical Security 17
   Why Worry About Physical Security? 17
   Physical Security Fundamentals 18

C. Social Engineering 21
   Why Worry About Social Engineering? 21
   Social Engineering Security Fundamentals 27

D. Email Security 29
   Why Worry About Email Security? 29
   Email Security Fundamentals 39

E. Untrusted Software 41
   Why Worry About Untrusted Software 41
   Software Security Fundamentals 43
Course Goals

The purpose of this security awareness course is to promote:

- Understanding of the value of information security.
- Understanding of the responsibility to protect the organization’s assets.
- Ability to recognize potential security risks and violations.
- Understanding of practices that promote computer security.
- Knowledge about whom to contact if you detect a security breach.

Course Objectives

Upon completion of this course, you will be able to:

- Identify the value of information to your organization and more specifically your department.
- Outline a responsibility tree that indicates responsibilities of various persons within your work group for protecting organizational assets.
- Describe common security risks and violations for computer users in the workplace.
- Describe the importance of password protection and techniques for creating strong passwords.
- Describe the importance of physical security and techniques for improving physical security in your work area.
- Describe social engineering risks and techniques for thwarting social engineering attacks.
- Describe email security risks and techniques for using email more securely.
- Describe the role of proper use.
- Identify whom to contact in the case of a security breach in your workplace.
Section 1: Understanding the Value of Information Security

“Everyone is familiar with the old adage “knowledge is power”. This saying has taken on new meaning in the information technology world. Why? Because with new information technology systems, more information is more readily available to more people. Information security has always been a concern, but the concern has been considerably heightened due to the advent of IT systems.

Computing and communications technology used to reside on standalone mainframes housed in the computing center. Therefore, security was the responsibility of the computing manager and staff. Today, computing and communications technology are distributed systems with terminals in individual offices and homes. As the systems themselves have become more dispersed, so too has the responsibility for security. Furthermore, many IT systems and products have been designed with ease of use and accessibility as primary functional requirements. You and I, as end users, think that is a good thing. However, from a security perspective, security can decrease as ease of use and accessibility increase. The aim of all information security is to create the appropriate balance between ease of use and security.

Did You Know…

“The goal is to ensure that everyone understands that protecting the enterprise is part of each person’s job.”


Did You Know…

“U.S. colleges and universities are ranked among the poorest protected systems because tightening security often means restricting access.”

So how does an organization strike the appropriate balance? The answer to this question varies from organization to organization, department to department, and person to person. The appropriate balance depends upon the need for confidentiality, integrity, and availability.

Confidentiality – how important is it that this information be protected so that unauthorized persons cannot access it?

Integrity – how important is it that this information be protected from intentional or accidental unauthorized changes?

Availability – how important is it that this information system be accessible by authorized users whenever needed?

On the following page there is an exercise for you to complete. In the space provided, give examples of types of information present in your workplace that must be kept confidential and potential consequences if it is not kept confidential. Then do the same thing for information integrity and availability.

---

Did You Know…

“The value of information, especially on original research, will eventually compel academic institutions to harden their defenses. ‘All it will take is a few well-publicized incidents of intellectual property theft to get the universities to lockdown their networks.’”

-Walsh, Lawrence.
Exercise #1: The Value of Information and Information Security in Your Workplace

Directions: give examples of types of information present in your workplace that must be kept confidential and potential consequences if it is not kept confidential. Then do the same thing for information integrity and availability.

<table>
<thead>
<tr>
<th>Types of Information that Must Be Secure</th>
<th>Potential Consequences of Poor Security Practices</th>
</tr>
</thead>
<tbody>
<tr>
<td>Confidentiality</td>
<td></td>
</tr>
<tr>
<td>Integrity</td>
<td></td>
</tr>
<tr>
<td>Availability</td>
<td></td>
</tr>
</tbody>
</table>
Section 2: Protecting the Organization’s Assets

There is no recipe that any organization can follow to protect its assets.....it requires a combination of well-created policies that are fully implemented. The policies and practices in place in any organization should be commensurate with the value of the information that must be protected and the impact of the failure to protect it adequately, as discussed in the exercise at the end of section 1.

Policies for information security should be derived not only from the information security needs of the organization and its users, but also from information security laws and regulations. Furthermore, it should be designed based on the information security needs of the various functions (departments, programs, sections, classifications, etc.) within the organization.

An effective information security policy is explicit, well thought out, comprehensive, fully implemented, evaluated regularly, and revised as needed. The following components are commonly found in information security policy and presented here to show you the big picture and specifically where user practices fit into the bigger scheme of information security policy.

1. Policy on Physical Controls, i.e., back up files and documentation, fences, security guards, badge systems, double door systems, locks and keys, biometric access controls, site selection, fire extinguishers, etc.

2. Policy on Technical Controls, i.e., access control software, anti-virus software, passwords, smart cards, encryption, audit trails, intrusion detection systems, etc.

3. Policy on Administrative Controls, i.e., security awareness and technical training, separation of duties, user registration, disaster recovery, contingency, and emergency plans, etc.
Note that security awareness and training is one initiative/program that is part of the larger policy undertaken to protect the organization assets. This training is one component of the security awareness and training program, which is part of administrative controls, which is part of information security policy as shown in figure 1.

Did You Know…

“Most companies have enough to do just taking care of their own business, never mind thinking about security.”


Figure 1. Elements of information security policy.
Exercise #2: Information Security Responsibility Chart

Directions: This is a two-part exercise. In part one, you need to draw and complete the chart to show the information security responsibilities of various persons in your organization. In part two, you need to specify who in your workgroup is responsible for protecting the assets that you identified in exercise #1. There is no penalty for leaving spaces blank.

Part 1

- Information Security Policy
  - Policy on Physical Controls
    Person(s) responsible: ____________________________
  - Policy on Technical Controls
    Person(s) responsible: ____________________________
  - Policy on Administrative Controls
    Person(s) responsible: ____________________________
Part 2

Go back to exercise #1. For each type of information that you indicated must be secure, list all of the people in your organization who are responsible for protecting each asset.

<table>
<thead>
<tr>
<th>Asset/type of information that must be secure.</th>
<th>List of all persons responsible for keeping it secure.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Section 3: Security Risks and Countermeasures

This section will cover the following 5 security threats common to computer users in the workplace:

- Passwords
- Physical Security
- Social Engineering
- Email
- Untrusted Software

After discussing each type of threat, you will be introduced to countermeasures that you can take to reduce your risk.
Section 3A: Password Basics

Why Worry About Passwords?

Passwords are often used to grant access to computer systems to approved parties. Likewise, passwords are often used as the first line of defense against unauthorized access. In the case of passwords, access is granted according to what you know, i.e., the password.

The fact is that users, for their own convenience, often pick passwords that are simple and easy to remember. Most users would like to pick one password, and 1) use it for all of their accounts, 2) use it all the time, 3) never have to change it, and 4) write it down so that they can reference it if they happen to forget it during vacation.

The problem is if the password is easy to remember, it is easy to guess. If the password is written down, guessing doesn’t even matter. And if the password is never changed, then repeated attacks are more likely to occur.

Many people also think it is inconvenient to have a timeout feature on their computer. Timeout features lock your account so that when you are away from your desk, other unidentified users cannot access your computer.

Passwords versus Pass Codes

Unfortunately, when the term password is used, it connotates exactly that with user, the notion of using a word to enabling passing the barrier to enter the system. Rather than think in terms of passwords, we prefer to think in terms of pass codes.

A code is a system of signals used to represent letters or numbers in transmitting messages. To create your own code, you might want to consider creating a pass phrase. A pass phrase is sort of like a personal algorithm. The phrase makes it easy for you to remember, but hard for someone else to guess.

For example: m+j=3rke This password represents the names of the people in my family. Melissa is my name, Jay is my husband, and we have three children, Rachel, Kate, and Erin.

2niletak This is one of my children’s names (Katelin) spelled backwards and she is the second of three children in our family, hence the 2.
Password Length and Possible Characters

The strength of your password is dependent upon the length of and the number of possible characters used in your password.

The formula for calculating the total possible number and letter combinations is:

\[ C = x^y \]

- \( y \) is the length of the password
- \( x \) is the number of possible characters
- \( C \) is the number of possible combinations

So if you are using numbers, you have the characters 0-9 as possible characters or 10 possible characters. If the password length is 4 characters, then the number of possible combinations is \( C = 10^4 \) or 10,000.

If you increase the possible characters to include numbers and all letters of the alphabet, then you have increased the number of possible characters to 36. For a password that is 4 characters long using 36 possible characters, the number of possible combinations is \( C = 36^4 \) or 1,679,616.

If you increase the possible characters to include numbers, all letters, and special characters (i.e., !, @, #, $, %, ^, &, *, and so on), then you have increased the number of possible characters to 68. For a password that is 6 characters long using 68 possible characters, the number of possible combinations is \( C = 68^6 \) or 98,867,482,624 (more than 98 trillion)!
Password Protection Fundamentals

The following are ten tips to help you select a password that is more secure, yet still relatively easy for you to remember.

1. **Use a minimum of 6 characters.**
2. **Use a combination of numbers (1-9), alphanumeric characters (A-Z), and special characters (!, @, #, $, %, ^, &,*,+,=).**

Try this on for size: Get>Sm@rt

If it is hard for you to remember special characters, create a common substitute that makes sense to you. For example, use $ as a substitute for s or S. Or use + as a substitute for t or T.

So instead of Get>Sm@rt, the password could be Ge+$mar+

3. **Don't pick a password that someone can easily guess.** What types of things are easy to guess? Here's a list of things that we advise you not use because they are easy to guess.

   - Don't use your login name in any form (as-is, reversed, capitalized, doubled, etc.).
   - Don't use your first or last name in any form.
   - Don't use your spouse's or child's name.
   - Don't use other information easily obtained about you. This includes license plate numbers, telephone numbers, social security numbers, the brand of your automobile, the name of the street you live on, etc.
   - Don't use a password of all digits, or all of the same letter. This significantly decreases the search time for a cracker.
   - Don't use a word contained in (English or foreign language) dictionaries, spelling lists, or other lists of words.

4. **Use a pass phrase.** A pass phrase is sort of like a personal algorithm. The phrase makes it easy for you to remember, but hard for someone else to guess.

   For example: The title of the song I Left My Heart in San Fransisco is a phrase that could be represented as the following password: EYELMHISF

   If you like the idea of using personal information in a pass phrase, consider the following passwords:
5. **Use a separate password for different accounts.** I know this makes it tough to remember multiple passwords. Try associating the password with the account. If you have an account to purchase books on line, use a pass phrase that is derived from a book title.

For example: Using the book title The Seven Habits of Highly Effective People could result in the following password: 7Hof^EP!

6. **Do not write down your password and leave it in an easy to view spot.** There isn’t much else to say here…..just don’t do it.

7. **Change your password regularly.** There is a temptation to recycle old passwords. You have two and you flip flop their use. Resist the temptation….it is too predictable.

8. **Do not give other people your password, intentionally or unintentionally.** While it might seem efficient to give your colleague your password so s/he can get a file off of your computer, who is to say that they will not write it down somewhere for ease of remembering. You also want to make sure that it is difficult for others to see you type in your password.

9. **Use the timeout feature to prohibit access when you are away from your desk.**

10. **Report any suspicious or abnormal circumstances to your system administrator as soon as you notice it.**
Exercise #3: Passwords, Passwords, Passwords

Directions: Using the guidelines provided, brainstorm and write down ten passwords that would be easy for you to remember, but hard for someone else to guess or crack. If you have multiple passwords that you have to use, try to create themes that you can use as well, but don’t write down which password is for which account….that wouldn’t be very secure. Be prepared to share with the class.

1. __________________________
2. __________________________
3. __________________________
4. __________________________
5. __________________________
6. __________________________
7. __________________________
8. __________________________
9. __________________________
10. __________________________
Section 3B: Physical Security

Why Worry About Physical Security?

With all the hype about viruses, hackers, and crackers, accompanied by the availability of firewalls, vulnerability testing, and intrusion detection, the physical security of computer systems is often overlooked. Unfortunately, many people do not realize the importance of physical security until it is too late.

Most people believe that the data on the computer is the most important thing to protect, but imagine if you came into work one day, and booted up your computer only to find that it did nothing. A quick check shows that the power is fine, but the computer is completely dead. You report this incident to the system administrator. Upon investigation, you learn that someone entered the box of the computer and stole your hard drive. Suddenly, the data you have been protecting is gone…..and not even a password would have protected it in this situation.

So don’t overlook the obvious. A skilled computer thief knows exactly what s/he is looking for and can make quick work of stealing hard drives, memory, CPU chips, and other components. While many of the required precautions for physical security are the responsibility of the system administrator, there are also basic physical security safeguards that every computer user should practice.
Physical Security Fundamentals

The following are six tips to help you create a physical work environment that is secure and protects your information assets.

1. **Lock up** – be sure to lock the facility when it is not being attended.

2. **Do not leave resources unattended during the workday.** Have you ever walked into an empty office in the middle of the day? I have many times. Usually everyone has a legitimate reason to be away from their desk whether it is due to an immediate meeting with the boss, last minute copies for a presentation, a crisis down the hall that required help, or an urgent bathroom break. Preventing physical loss during these times requires two things:
   
   A) Awareness that you are at risk, and
   
   B) A willingness to work as a team and communicate to ensure that the office is not left unattended.

   Did You Know…

   “The cost of replacing the device is quite irrelevant in comparison to what the device holds.”


   Create a schedule for office coverage so that someone is in the office at all times. Then during times of emergency, be sure to communicate with others to let them know if you need to be away during your scheduled time.

3. **Know whose responsibility it is to lock up.** While this might seem overly simple, sometimes the simplest things are the easiest to overlook. The time when this becomes especially important is when the person who normally locks up goes on vacation, is sick or away from work for other reasons. Now all of the sudden, someone in the office has to fill in for the person who normally locks up. The person filling in is usually trying to do two jobs at once. And, considering the fact that we all get busy and used to our routine, it is easy to see how doors get left unlocked.
4. Do not grant unauthorized people access to equipment. Many workplaces have become very reliant upon computer and information systems to conduct business. I know, firsthand, the frustration of lost productivity due to the computer system being down. It is easy to understand why we want our computer and information systems available for use ALL THE TIME. However, the need for constant availability sometimes can put the organization at risk.

People who want access to your computer system know that businesses have become increasingly more reliant upon their computer systems. They also know that they can play on this reliance by posing as system auditors, certifiers, administrators, etc., to gain access. And lastly, they know how to create the proper identification to convince others that they are authorized to access the equipment. So it is also important that you know how to confirm 1) that an individual really does have authorization and 2) exactly what they have authorization to.

This topic will be discussed in greater detail in Section 3: Social Engineering. The bottom line is this: Do not grant access to unauthorized persons and know where and how to confirm authorization.

5. If you are in an open area, request a security cable for your equipment. After all, it is harder to walk out with something that is tied down than something that’s not!
6. If you use a laptop, keep it close by at all times. Consider the following story:

Did You Know…

“Laptop theft is a growing problem – one insurance company says that nearly 320,000 laptops valued at $800 million were stolen in 1999.”


Case in Point

The personal portable computer of Dr. Irwin Jacobs, Qualcomm’s chief executive officer disappeared from a hotel conference room moments after Dr. Jacobs addressed a national business journalists’ meeting. Qualcomm is a leader in developing, delivering, and enabling innovative digital wireless communications products and services. The laptop contained proprietary information that could be valuable to foreign governments. How did it happen? Dr. Jacobs left the computer unattended on a podium for about 15-20 minutes when he stepped down to talk to a small group of business Editors and Writers less than 30 feet away.

While you might not have proprietary information on your laptop, this story points out just how easy it is to steal laptops and how important it is to keep them close by.
Section 3C: Social Engineering

Why Worry About Social Engineering?

To understand why it is important to worry about social engineering, you have to first understand what social engineering is in the world of Information Assurance and Security. Basically, social engineering is the art and science of getting people to comply with your wishes. The aim of many social engineers in the world of Computer and Information System Security is to trick people into revealing 1) passwords or other information that compromises a target system’s security, 2) credit card numbers or other personal information that compromises the individual, or 3) to gain access to unauthorized areas where equipment is stored.

The fact is that all computer systems rely on humans. Humans turn on computers. Humans create passwords. Humans enter credit card numbers. Therefore, the human part of security is independent of platform, software, hardware, networks, and so on. This makes human beings a universal weakness in Information Assurance and Security. An individual experienced with social engineering techniques can practice this form of hacking wherever s/he goes.

Social engineering is performed in a variety of ways and you should be aware of all of them. The four predominant methods include: 1) over the phone, 2) via the Internet, 3) snail mail, and 4) in person. In addition, you should be aware of some of the psychological factors at play. Let’s look at each of these in greater detail.

1. Telephone: The telephone is the most common means for social engineering. Why? Because it is easy, quick, and fairly cheap. Common scams include posing as the internal system administrator, the local phone company technical support, and so on. Consider the following true story:

Did You Know…

“Kevin Mitnick, the well-known hacker that cost companies like NEC USA, Nokia, and Sun at least $290 million over a two-year span, sometimes didn’t have to hack at all to defeat computer defenses. Using what’s known as social engineering he was often able to get people to give him their passwords or whatever he needed to break in to a network.”

Jack was a Computer Engineer with a masters degree. In December 1995 he got a phone call from Phillip Smith who identified himself as a customer service representative of New Mexico Internet Access.

Phillip started the conversation by saying “We’re calling all of our customers to let you know that we have decided to start accepting credit card payments on your account.” Jack reports thinking this was a great idea because New Mexico Internet Access had a terrible billing procedure. They did not use credit cards and they didn’t send you a bill each month, not even by email. They relied upon the customer to remember to pay their access fee. If the customer failed to remember, the penalty was cancellation of their account. One day you try to dial up and “nada”, nothing….no Internet access.

Now while this may sound strange to you, at the time no one thought much of it. This was the dawn of the commercial Internet, there were very few ISPs and people were just glad to have access.

Jack hesitated. Sensing his reluctance, Phillip added “Because this will guarantee and simplify billing, we will cut your monthly bill from $20.00 to $15.00, if you go to credit card payment”.

That was all it took. Jack took the bait, hook, line, and sinker. The next month charges for computer games turned up on Jack’s credit card statement. Not to mention that New Mexico Internet Access cancelled his account for lack of payment.
Social Engineering over the telephone often makes use of equipment. The following quote is from a website written by a social engineer who goes by the name Meinel. It reads as follows:

“The phone should be of good quality and try to avoid cordless, unless you never get static on them. Some phones have these great buttons that make office noise in the background. Caller ID units are helpful if you pull off a scam using callback. Something else I use is a voice changer. It makes my voice sound deeper than James Earl Jones or as high as a woman. This is great if you can’t change your voice very well and you don’t want to sound like a kid. Being able to change gender can also be very helpful.”

2. Internet: The Internet can also be a tool for social engineering. While many of the schemes on the Internet fall into the realm of hacking, when the means used to garner information on the net include scheming a person into divulging information, then it is still considered social engineering.

Common scams include posing as someone you are not via emails and chatrooms. The true example on the next page describes an email message sent to America Online customers that directed them to a copy cat website to collect user names, passwords, and credit card numbers.

Did You Know…

“The IloveYou virus was the first to use the social aspects of viruses. Because of its friendly message, experts said, and the fact that it ‘came from’ a familiar person, the virus writers increased the odds a user would open the VBS payload.”

Dear America Online Member,

We’re sorry to bother you during the holiday season. However, with the change to the new millennium, thousands of hackers are taking advantage of the Y2K bug. America Online is taking a great amount of action and preparing for the worst. We need you to provide your current billing information by clicking <A HREF="http://verifybilling.cjb.net">here</A>. If you do not complete this form before you sign off today, your account will be suspended until you contact us directly with this information.

Sincerely,

Bill Fieldhouse, Billing Department,
Representative Identification # 103

3. **Snail Mail:** Regular U.S. mail service can also be an effective means for social engineering. It is effective for the person trying to get information because it is cheap and also because people tend to trust the written word.

A particularly effective way to get personal information is by simulating a sweepstakes. After all, it is hard to resist filling out a sweepstakes form.

The information that the social engineer is after might be your name and your Internet service provider, your name and your email service provider, etc. With that in hand, they are well positioned to call on you later and pose as the system administrator for your Internet Service provider. These scams can be elaborate, using more than one method to gain access to confidential information.
4. **In Person:** While it takes more time and effort for the hacker, sometimes social engineering must be done in person to get the needed information. People tend to trust people whom they can see. It is much easier to build a sense of trust in a person than it is via faceless communications. And most of us are trusting – it is human nature.

Because you can build a greater sense of trust in person, the goal of social engineering done this way is not just to gain access to a password, but to gain access to the entire system, i.e., the equipment room.

According to social engineers, a particularly effective method for in person social engineering is by posing as a trusted authority figure. For example, posing as the fire marshal, or as a security supervisor. Consider the following example:

A hacker posing as the fire marshal gains access to the public access areas including the company lunchroom. The local spa/exercise facility has an advertisement in the lunchroom. According to the ad, everyone who leaves a business card is eligible for one week of free membership to the spa, and one lucky winner will be chosen every month to receive three months of free membership. The hacker finds the jar full of business cards, sorts through them, and selects a few. S/he then takes them to a print shop, where business cards are made using a fake name and title.

Two months later the hacker returns to the company and announces her/himself to the receptionist......business card in hand. Assuming the card is legitimate, she issues the hacker a building pass.
Another mechanism for gaining access to confidential information is called dumpster diving. Discarded pieces of paper with passwords are among the many types of confidential information that can be found in the trash.

**Psychological Ploys:** An effective social engineer goes into every situation with a plan for how they are going to obtain the desired information.

While this is not an exhaustive list, the following psychological ploys are purposefully used by social engineers because of their effectiveness: 1) diffusion of responsibility, 2) ingratiation, 3) moral duty, and 4) conflict avoidance.

1. Diffusion of Responsibility: a social engineer will often look for ways to make the target perceive that they will not be responsible for their actions. Once relieved of personal responsibility, target’s are much more likely to share information.

2. Ingratiation: social engineers know that compliance is more likely if the target believes that by complying they are ingratiating themselves with someone who may give them future benefits....basically getting in good with the boss.

3. Moral Duty: this is where the individual complies because they feel it is their moral duty. Sometimes this is conveyed as being able to feel a part of a greater good cause and sometimes it is a message of guilt for doing nothing.

4. Conflict Avoidance: this is where the target complies in order to avoid conflict. On the whole, people do not like conflict and will often take actions to avoid conflict and/or to resolve it.
Social Engineering Security Fundamentals

The following are six tips to help prevent you from becoming the target of a social engineering attack.

1. **Realize that computer security is a part of everyone’s job.**

2. **Awareness of social engineering.** An effective and wise precaution against social engineering is knowing basic methods for social engineering, as presented in this manual.

3. **Do not give out confidential information without verification.**
   - Network administrators do not need to know your password. If you are ever asked for your password, it is probably a social engineering attack.
   - Do not share your userid and password with anyone.

4. **Verification, verification, verification!**
   - Verify that the person is who s/he says s/he is….on the phone and in person.
   - Verify that the business that the person says s/he is from is a real company.
   - Verify that the person actually works at that company.
   - Verify that the url matches the one you are familiar with.
   - Verify that the person is supposed to be working on the equipment.

5. **Do not put confidential information in the trash without shredding it first.**

6. **Report any suspicious behavior to the system administrator immediately.**
Exercise #4:  Social Engineering Case Study

Directions:  Read the following case study and questions.  Be prepared to discuss the case study in a small group discussion.  Assign one person in your group to be the recorder.  The recorder should write down the answers to the questions that the group discusses to present to the class.

Three weeks ago Eastern College was hacked.  The computer hacker posed as a system administrator for the school and called a clerk in the registrar’s office.  The conversation went something like this:

Hacker: “Hi, this is Daryl with tech support.  We have had some folks in your office report slowdowns in logging in lately.  Is this true?”
Clerk: “Yes, it has seemed slow lately.”
Hacker: “Well, we have moved you to a new server, so your service should be much better.  If you want to give me your password, I can check your service.  Things should be better for you now.”

Unfortunately, Daryl did not really work in tech support at Eastern College.  Daryl hacked into the registrar’s system, from there he found the bursar system.  Eastern College had started accepting credit card payment two years earlier.  Within four weeks, over 30% of the students and/or their parents reported that their credit card numbers had been stolen and used.

Questions:

1. What might be the consequences of this incident for Eastern College?
2. How easy would it be for something like this to happen in your place of work?
3. How would you propose preventing incidents like this from happening in the future?
Why Worry about Email Security?

Email has been likened to postcards. Why? Because both email and postcards are easy to intercept. And if intercepted, both are easy to read, and/or change. By its very nature, all email is insecure. Furthermore, email costs little to nothing, so millions of people have it. For these reasons, email is an accessible method for exploitation.

You might think, “It’s only email, why should I care?” There are several reasons you should care, and hopefully these will become apparent to you in this section. The insecure aspects of email manifest themselves in different ways. The following list will explain to you, in lay terms, issues associated with email that make it insecure.

1. Privacy – when you send an email message, your message passes through various networks as it travels to its final destination. This is somewhat similar to the U.S. Postal Service in that a letter that you mail goes through many different post offices before it reaches its final destination.

However, U.S. Mail is regulated so as the letter passes from post office to post office the same set of policies apply. The outcome, of course, is that the mail is more secure than it would be if we did not have uniform policies system wide. Well, email travels over the Internet, which is not regulated. As the email passes from one network to the next, there is no standard that regulates the level of security required on the network.

The information in the box on the top of the next page shows you the networks (“mail stops”) that a recent email of mine traveled through to get to me from the sender. The networks are shaded. As you can see, this email message traveled through seven networks.
Each node is a potential security risk. Email can be read by anyone who is able to access any network between you and the person you are sending mail to. The only way to ensure that your email is not read by others is to encrypt it. However, there are many less technical things that you can do on a regular basis to reduce your email security risk.
2. Spam – this is the Internet version of junk mail. A spam email is generally defined as an unsolicited mailing, usually to many people. A message written for, and mailed to, one individual that is known to the sender is not spam, and a reply to an email is not spam, unless the "reply" repeats endlessly. Spam emailers have become a separate part of the Internet, with their own host computers, methods, and politics.

According to the Gartner Group, a research firm, about 90% of email users receive spam. It is prevalent and expected to grow. Why be concerned about spam? Actually there are several reasons why you should be concerned.

A. It is costing money. The recipient of the advertising is forced to pay the cost of the message. Your organization pays for email for various reasons, but not for you to receive advertising. It is costing the organization real money in terms of extra connection-time charges, phone time charges, disk space, and lowered bandwidth.

B. It results in lost productivity. Junk email wastes valuable time, because you have to spend extra time to download the unwanted messages, and then to wade through the junk email in order to get to the email you actually want.

C. Junk email clogs up people’s email boxes, mingling with and sometimes even preventing receipt of legitimate email.

D. It may cause employers to pull employee internet email access, because they don't want to pay money for their employees to receive advertisements, nor for the lost productivity of their employees wasting (employer-paid) time identifying and discarding junk email.

E. It discourages people from participating in the Internet.

F. Spam is growing every day. As it continues to grow, the problems mentioned above will only worsen. The following story provides a glimpse of how spammers are facilitating the growth of spam on the Internet.

A friend of mine conducted a small experiment. She got unsolicited commercial email with the usual message: "If you don't want to receive future email from us, use the REPLY button and place the word CANCEL in the subject header." My friend created a new email account, and used it to reply to the UCE. That email account was almost immediately flooded with a large number of UCE, not just from the first offender, but from others as well. So it appears that this REPLY solution is just another scam to collect addresses with which to further clog the net.
While spam comes in many different disguises, let’s take a minute to look at some of the more frequently used and abused methods for spamming.

Chains - Chain letters are letters that promise a phenomenal return on a small effort. The return might be the promise of a free product or service, luck, love…..you name it, they will think of it. You are supposed to send the letter or some other thing on to other people. If you send it on, you will then get the promised in return. If you do not send it on, then you will get nothing in return or potentially suffer some type of harm. Here are a couple of classic examples.

Hello Everyone,
And thank you for signing up for my Beta Email Tracking Application or (BETA) for short. My name is Bill Gates. Here at Microsoft we have just compiled an email tracing program that tracks everyone to whom this message is forwarded to. It does this through an unique IP (Internet Protocol) address log book database. We are experimenting with this and need your help. Forward this to everyone you know and if it reaches 1000 people everyone on the list will receive $1000 and a copy of Windows98 at my expense. Enjoy.

Note: Duplicate entries will not be counted. You will be notified by email with further instructions once this email has reached 1000 people. Windows98 will not be shipped until it has been released to the general public.

Your friend,
Bill Gates & The Microsoft Development Team.

Did You Know…

Netcom estimates that approximately 10 percent of its customers' monthly bill is devoted to fighting SPAM.

Internet Week, May 4, 1998

Did You Know…

SPAM is estimated at more than 25 million emails per day or roughly 10 percent of all email world-wide.

This is a promise, send back to make the promise...

You are my friend and I hope you know that's true.
No matter what happens I will stand by you.
I'll be there for you whenever you need.
To lend you a hand to do a good deed.
So just call on me when you need me my friend.
I will always be there even to the end.

Forward this promise to all your friends to show your friendship and watch who sends it back.

Hoaxes – an email hoax is a specific type of chain letter that deceives you in order to prompt you to pass it along. Frequently email hoaxes pose as an alert and use technical jargon. This is done on purpose to confuse readers and to make them feel as if they are doing a service by passing the hoax email along. Anyone who sends these is doing just the opposite. The most common manifestations of hoax chain letters are phony virus alerts and appeals to fighting medical diseases. See the following examples.

If you receive an email titled "WIN A HOLIDAY" DO NOT OPEN IT. It will erase everything on your hard drive. Forward this letter out to as many people as you can. This is a new, very malicious virus and not many people know about it. This information was announced yesterday morning from Microsoft; please share it with everyone that might access the internet. This was sent to us by Jan Truskolaski at Lucent Technologies. Please, pass this along to everyone in your address book so that this may be stopped.
For cardiomyopathy research...Tickle me! :-) 

For every new person that this is passed on to The American Heart Association will donate 3 cents to heart disease research. Please help us. Forward this to everyone you know. Thanks for helping!!
Rebuttals – the rebuttal is disguised as an attempt to combat chain letters, but in fact is a chain letter itself. A clever way to appeal to those who have grown very tired of chain email. Here is an example of this type of chain letter.

To Whom It May Concern:

This letter is being sent to you because recently, you were sent a chain letter, which you may or may not have passed on. This is an anti-chain letter. It originated at Portland State University. Its purpose is to put a stop to all of the silliness of chain letters and their complete lack of connection with luck, fortune, or anything else. If you receive this anti-chain letter, keep it until you receive a chain letter. Then instead of spreading the chain letter, send this letter back to whoever sent that obnoxious piece of junk mail to you.

If you sent one recently, send this along to the same people. If we get lucky, maybe this will spread all over the world and eventually get back to those goobs who have nothing better to do than write meaningless letters that prey on people's superstitions. (How do they know how many times a letter has been "around the world" anyway?)

If you don't, your car will not break down; a close relative is not going to die; and you won't lose all of your money. If you do, you probably won't win a million dollars, receive a promotion, or suddenly find true love. (We sincerely hope you do anyway.) However, you will feel much better about ignoring chain letters in the future.

Thank you.
3. Information Leaks – sending out confidential information of any kind on email can be harmful. Given our conversation about networks and spam, you might be thinking that you only have to worry about email that uses the Internet; and that internal email that travels over your organization’s Intranet is secure. In fact, you do have to worry about internal email....according to many experts, the biggest threat comes from within an organization. Consider the story on page 24.

Frank was not performing on his job and felt that his boss, Mark, was out to get him. Over the course of six months, Frank had several meetings with Mark. With each meeting that took place, Mark was using disciplinary actions that were progressively more serious. At their last meeting, Frank received a written warning. The warning spelled out performance expectations for Frank for the next month. It also specified that if Frank did not perform up to expectations, that he would be fired. Frank knew his job was on the line.

Five months earlier when all this began, Frank had been working on a special project with Nina, one of the Administrative Assistants in Human Resources. Nina was fairly new to the company and this was the first time she had performed some of her work on a computer system. Nina and Frank had regular scheduled meetings to work on the project. However, Nina woke up with a fever one morning and called in sick. Frank, being a pretty shrewd guy, called Nina at home and volunteered to complete the task on his own. There was just one small problem, he would need access to the files, which were on her computer. Without hesitation, Nina gave Frank her userid and password, and thanked him for volunteering to do it by himself.

With termination pending, Frank began to intercept and read all of Nina’s email. After about two weeks, Frank intercepted an email from Nina’s boss to Nina indicating the official date of Franks termination...... Friday, the 15th. Frank came in to work early that morning and executed a program that would start running one week later. The program, which destroyed several financial records and the customer order database, wreaked havoc on the company.

Did You Know...

“80 percent of firewall breaches are due to internal causes, whether a disgruntled employee or an honest mistake.”

4. Tampering – in addition to intercepting email for purposes of accessing confidential information, sometimes the underlying motive is for gain or harm by actually tampering with the message. If it is a case of tampering, then the message that is received will be different from the message that was originally sent.

In the case of a spoofed email, the message will appear to be from one person, when in fact, it is from an entirely different person.

5. Offensive contents – proprietary or confidential information is not the only kind of content that you should be concerned about when it comes to email. Offensive material can be equally troublesome. Offensive content would include, but is not limited to, sexual comments or images, racial slurs, gender-specific comments or any comments that would offend someone on the basis of his or her age, sexual orientation, religion or political beliefs.

6. Viruses – due to viruses such as Melissa, Y2K, and the Lovebug, it is fairly wide known that email is used to spread viruses. The effect of a virus passed via email can range from simple annoyance to serious destruction.

Viruses are often spread via attachments. If your organization does not allow the use of attachments, this is probably why. As a user, you usually will not know that you have received a virus until you have opened the attachment. At this point, it is too late to keep from being infected. The act of opening the attachments activates the virus; it is now infecting your hard drive and possibly the network.

Viruses can also be transmitted via macros. Macros are tiny programs written to carry out actions. They are used to automate frequently performed tasks, such as addressing a letter to multiple recipients. Macro viruses are application specific and are most commonly found with applications such as Word, Excel, PowerPoint, and Access. The Melissa virus was a macro virus whose carrier was Microsoft Word 97 or Word 2000. If you received an infected document that you opened using another application, such as WordPerfect, you would not be infected with the virus. However, if you received an infected word document, and subsequently opened it with word, you can be infected if macros were enabled on your machine.

---

**Did You Know…**

“In the scant few hours it took to develop a patch to defeat the IloveYou bug, the amorous worm had copied and distributed itself to some 10 million computers. Experts disagree on the total damages, but estimates range from $700 million to $15 billion.”

Sophisticated viruses are able to open your personal address list and send themselves on to everyone in your address book. This is an important point because it implies that sometimes you cannot even trust email that comes from a known source.

In addition to being embedded in .doc, .xls, and .ppt files, viruses are commonly transmitted in the following file types: .exe, .vbs, and .shs.
**Email Security Fundamentals**

Email poses a significant risk to security. One of the most effective tools for counteracting this security risk is an educated workforce and sound policy. The following tips will help you be more secure in your email use and practices.

1. **Minimize the use of attachments.** Copy and paste text as often as possible.

2. **Question unsolicited documents.** Unsolicited bulk mail and commercial email can put you and your organization at risk. Questioning it means not opening it, not passing it on, and notifying your system administrator immediately.

3. **Never respond to spam email.** For a spammer, one "hit" among thousands of mailings is enough to justify the practice. Instead, if you want a product that is advertised in a spam email, go to a Web site that also carries the product, inquire there, and tell them you do not approve of spam methods and will not patronize a company that uses spammers.

4. **Never respond to the spam email's instructions to reply with the word "remove."** This is just a trick to get you to react to the email -- it alerts the sender that a human is at your address, which greatly increases its value. If you reply, your address is placed on more lists and you receive more spam.

5. **Never sign up with sites that promise to remove your name from spam lists.** These sites are of two kinds: (1) sincere, and (2) spam address collectors. The first kind of site is ignored (or exploited) by the spammers, and the second is owned by them. In both cases your address is recorded and valued more highly because you have just identified it as read by a human.

6. **Do not include confidential information in email.** It does not matter if the information pertains to you or someone else, and it does not matter if the email system is Internet or Intranet based, confidential information in email is a risk that is not worth taking.

7. **Do not include offensive information in email.**

8. **Question executable programs received via email.** This is a common means for passing on viruses. Do not open them, do not
pass them on, and notify your system administrator if you receive them.

9. **Disable macros on your machine.** To do this, you will need to open the application. On Word 2000, select **Tools**, then select **Macros**, then select **Security**, and then check **High**: Only signed macros from trusted sources will be allowed to run. Unsigned macros are automatically disabled.

10. **Make sure that file extensions are viewable.** This will alert you to files of the following types: .exe, .vbs, and .shs. To view file extensions in Windows select the **Start** menu, then select **Settings**, then select **Control Panel**, then select **Folder Options**, then select **View**, then **UNCHECK** the command that reads **Hide File Extensions for Known file Types**.

11. **Notify the person you received an infected email from.** This helps them correct the problem within their system before passing the virus on to other users.
Section 3E: Untrusted Software

Why Worry about Untrusted Software?

Because it is untrusted, right? The hard part is differentiating between trusted and untrusted software. Obviously, we know that the software we buy from the local store that comes sealed with a shrink wrap and was produced by a legitimate company is “trusted.” But we all like freeware and shareware that we can download from the Internet. Now we are faced with a different situation.

How can we verify that the software is safe? How can we verify that the source is a trusted source and therefore their software can be trusted. Furthermore, how can we verify that the software comes from whom it is supposed to be coming from and not an imposter?

Actually, the effects of untrusted software have already been referenced several times in this manual. However, we have not specifically identified all types of untrusted software yet. We will do that now. This section defines malicious software. Some of it will be review of concepts and concerns discussed earlier. Some of it will be new terms and definitions.

What is a computer virus?

A computer virus is a program that requires a host in order to make copies of itself on computer disks. Viruses may infect (copy to, and spread from), program files, programs in disk sectors, and files that use macros. The ability to self-replicate distinguishes viruses from programs that do not, and this parasitic nature is neither an accident, nor a computer glitch. All viruses are created by people who know how to write computer programs.

The first theories about the possibility of creating a self-replicating program date back to 1949, and experimental viruses were first programmed and tested in the 1960s. They got their name when a university professor used the term “virus” to describe them 1984, because like a biological virus, a computer virus is small, makes copies of itself, and cannot exist without a host. When personal computers became popular, PC viruses began to appear (in 1986-1987), at first intended as jokes, or developed for research or demonstration purposes.
What is an armored virus?
An armored virus tries to prevent analysts from examining its source code. The virus may use various methods to make tracing, disassembling and reverse engineering its code more difficult. A good example is the Whale virus.

The term armored virus actually comes from the medical field. Anyone suffering from a cold knows how tough and persistent viruses can be. Scientists have discovered that one type of virus actually comes equipped with an armored coat made of interlocking rings of protein. The structure of this virus is remarkably similar to chain mail suits worn by medieval knights. The head of the virus is organized exactly like medieval armor, referring to the chain mail suits worn by knights in the Middle Ages. These protective outfits were made of interwoven rings of iron that were designed to deflect arrows while allowing maximum freedom of movement during battle.

What is bacteria?
Electronic mail that spreads itself to all users when read or otherwise executed.

What is a chain letter?
Electronic mail that spreads similarly to real chain letters. You send a letter to ten people, who also send it to ten people, and so on. In addition, electronic chain letters can use your address book to spread themselves……something that physical chain letters could never do!

What is a cuckoo's egg?
A program that you maintain and nurture on your system, which you believe is yours, but is actually someone else’s. The program is a malicious program and will eventually do evil.

What is a logic bomb?
A logic bomb is a type of trojan horse that executes when specific conditions occur. Triggers for logic bombs can include a change in a file, by a particular series of keystrokes, or at a specific time or date. See: Time Bomb.

What is malicious code?
A piece of code designed to damage a system or the data it contains, or to prevent the system from being used in its normal manner.

What is malware?
A generic term used to describe malicious software such as: viruses, trojan horses, malicious active content, etc.
**What is a master boot sector virus?**
Master boot sector viruses infect the master boot sector of hard disks, though they spread through the boot record of floppy disks. The virus stays in memory, waiting for DOS to access a floppy disk. It then infects the boot record on each floppy disk DOS accesses. Also: Master Boot Record Virus.

**What is a rabbit?**
A program that replicates itself very quickly.

**What is a resident virus?**
A resident virus loads into memory and remains inactive until a trigger event. When the event occurs the virus activates, either infecting a file or disk, or causing other consequences. All boot viruses are resident viruses and so are the most common file viruses.

**What is a self-garbling virus?**
A self-garbling virus attempts to hide from anti-virus software by garbling its own code. When these viruses spread, they change the way their code is encoded so anti-virus software cannot find them. A small portion of the virus code decodes the garbled code when activated. Also called: Self-encrypting Virus, Polymorphic Virus.

**What is a time bomb?**
A program that is written so that it occurs on a specific date, and/or time. For example: The Y2K bug, a virus written to execute on the January 1, 2000.

**What is a Trojan horse?**
Trojan horse programs are named for the giant wooden horse that concealed Greek soldiers who used it to invade the ancient city of Troy. Like that famous trick, a Trojan horse program conceals hidden programming. The hidden function may just be a joke, or something annoying, but vandals often use Trojan horse programs to destroy other people's data, knowing that some people will run any program that has an interesting file name, or promises to perform a useful function. A Trojan horse is a program that appears to be one thing, but is something entirely different. Many people use the term to refer only to non-replicating malicious programs, thus making a distinction between Trojans and viruses.
What is a virus?
A program that infects other programs by modifying them to include code that instructs other computers to replicate the virus to still more computers. Viruses are capable of mutating or changing while they are replicating themselves. This is one reason why fighting viruses is particularly difficult. Viruses can be benign or malignant. Malignant viruses seek to destroy your data, files, or system. Benign viruses seek to cause disruption, but not destroy.

What is a virus hoax?
Hoaxes are not viruses, but are usually deliberate or unintentional e-messages warning people about a virus or other malicious software program. Some hoaxes cause as much trouble as viruses by causing massive amounts of unnecessary e-mail.

Most hoaxes contain one or more of the following characteristics:

- Warnings about alleged new viruses and its damaging consequences,
- Demands the reader forward the warning to as many people as possible,
- Pseudo-technical "information" describing the virus,
- Bogus comments from officials: FBI, software companies, news agencies, etc.

If you receive an e-mail message about a virus, check with a reputable source to ensure the warning is real. Visit McAfee.com’s Virus Hoax page (http://vil.mcafee.com/hoax.asp) or with Vmyths.com a website about virus hoaxes (http://www.vmyths.com) to learn about hoaxes and the damage they cause. Sometimes hoaxes start out as viruses and some viruses start as hoaxes, so both viruses and virus hoaxes should be considered a threat.

What is a worm?
As intranets and the Internet have grown in popularity, e-mail has evolved from a convenience to a necessity. Virus vandals know that, and they’ve invented new ways to use e-mail to spread viruses, and especially, worms. A worm program is similar to a virus. It is considered by some to be a subset of a virus in that it makes copies of itself but does so without needing to modify a host. Like viruses, worms may (or may not) do things other than replicate. A worm will eventually use all the memory in a computer or network.
What is in the wild?
In the wild is a term that indicates that a virus has been found in several organizations somewhere in the world. It contrasts the virus with one that has only been reported by researchers. Despite popular hype, most viruses are "in the wild" and differ only in prevalence. Some are new and therefore extremely rare. Others are old, but do not spread well, and are therefore extremely rare. Below is a list of those thought to be "in the wild".

The Inception of Computer Worms

On Nov 2nd 1988 Robert Morris Jr., a graduate student in Computer Science at Cornell, wrote an experimental self-replicating, self-propagating program called a worm and injected it into the Internet. He chose to release it from MIT, to disguise the fact that the worm came from Cornell. Morris soon discovered that the program was replicating and reinfecting machines at a much faster rate than he had anticipated - there was a bug. Ultimately, many machines around the country either crashed or became "catatonic". When Morris realised what was happening, he contacted a friend at Harvard to discuss a solution. Eventually, they sent an anonymous message from Harvard over the network, instructing programmers how to kill the worm and prevent reinfection. However because the network route was clogged, this message did not get through until it was too late. Computers were affected at many sites, including universities, military sites and medical research facilities. The estimated cost of dealing with the worm at each installation ranged from $200 to more than $53,000. Robert T Morris was convicted of violating the Computer Fraud and Abuse Act (Title 18), and sentenced to three years of probation, 400 hours of community service, a fine of $10,050, and the costs of his supervision.
Are all these programs harmful?
They waste disk space and memory, delay computer operations, and increase the likelihood of system crashes. They are often poorly written and may function erratically, overwrite data, and cause programs to run erratically. Many also have destructive routines to alter or overwrite data. In addition, the cost of antivirus software and the time recovering from virus damage is passed along to consumers by businesses at the cash register.

Who creates these programs - and why?
Virus writers range from researchers, to pranksters, to malicious vandals. The typical virus writer is an otherwise intelligent male, between 15 and 23 years old. He may be bored, curious, or intent on doing forbidden things, just to frighten others. Some belong to organized virus-writing groups (usually short-lived), and those in the group often respond to peer pressure, trying to outdo the others. Whether in a group or not, some get satisfaction from the challenge, while others think of themselves as rebels against the "system."

How do they spread?
Viruses and Trojans spread from one computer to another by using one or more methods, all of which depend on user carelessness. Some people never have a problem, but others who are not as careful (or lucky) infect their hard disk by running downloaded files, or after placing a newly-obtained floppy disk in a drive. Viruses and worms spread fastest among computers networked on a LAN, especially when e-mail file attachments are involved.

Is sharing files a problem?
Sharing certain types of files with others always involves some certain risk. The medium is irrelevant; files from a LAN server, downloaded from Internet sites, from a floppy (even from shrink-wrapped software). Riskiest of all are files posted on Internet newsgroups, because there is no control or accountability. Many people have become the first victims of brand-new viruses and worms, by downloading executable files that were posted deliberately by vandals.

What about e-mail?
Before the growth of the Internet, viruses used to spread more slowly, from user to user, and anti-virus vendors were usually able to distribute a remedy before things got out of hand. That's all changed, especially with worms, because some people will click on any e-mailed file that they receive. Vandals have seized their opportunity, and created programs designed to spread to all those who correspond with careless users. Because of this threat, the only 100 percent safe e-mail file attachment is a deleted e-mail file attachment.
Can a cookie contain a virus?
Some Web sites store information on your computer, in small text files called cookies, that can be used when you re-visit that site. Examples include items you've selected for purchase, registration data, or your user name and password, for Web sites that require them. Since cookies are text files, they are not executable, and this fact eliminates the possibility of viruses, because they must be hosted by an executable file. It is theoretically possible to include UUencoded or MIME comments, but decoding a UUencoded or MIME file and executing it is not possible.

How can you tell whether your computer is infected?
Because some viruses cause strange things to happen, an odd or unexplained event may lead a user to conclude a virus must be responsible, without bothering to explore other possible causes. On the other hand, many viruses are carefully programmed to do nothing to betray their presence. The solution to this dilemma is not to assume anything, but to rely upon anti-virus software as a diagnostic tool.

How can you protect your data?
If you have files you can't afford to lose, make sure you have more than one copy of them. Programs may already be backed up on their original installation disks, but what about the files that you create? Business records, spreadsheets, manuscripts, and other important files can be lost in an instant to a virus, or to other causes, hard disk failure among them. If no other copy of your files exists, make copies of them, before it's too late.

Do you need to worry?
Worrying will get you nowhere. Instead, take sensible precautions, to avoid losing data should you be affected by a program that was designed to cause problems. Many people are fortunate never to encounter one, but a vandal's program could be concealed in the next file you download, or in a file attached to an e-mail message. Or the threat could be on the next floppy you insert in a disk drive, especially one obtained from a friend, a co-worker, or a fellow student.
Software Security Fundamentals

So, what can YOU do to secure yourself from untrusted software? There are many things that you can do, some of them we already talked about, so they are mentioned very briefly here. The good news is that most of these preventive measures are relatively easy to do.

1. Do not download executable programs from bulletin boards. Bulletin boards are a launching pad for untrusted software.

2. Do not accept or use unlicensed software. Legitimate businesses are just that, legitimate….for the most part, they are on the up and up.

3. Do not share software disks with other users freely.

4. Do not allow access to your computer by people whom you do not trust.

5. Do not leave your disks unattended.

6. Do not ignore abnormal functioning of your computer…..it might be symptoms of a virus or other malicious software.

7. Back up essential files. Keep a log of what you do to learn which applications are most important to you. Although you can restore them from their installation CDs, that does not mean they'd work the way they do now. So if you have re-configuration any, you'd need to find out how and where they store that data, in order to back it up.

Make backup copies of files on your hard disk. All hard disk files would be best. Some files may already be backed up (in effect) on original installation disks, but most important are the files you create with your applications. Business records, spreadsheets, manuscripts, and other important files that take tremendous work to produce can be lost in an instant--if no other copy exists. Do not take that risk--make copies of them.

8. Delete e-mail file attachments. The only 100 percent safe e-mail file attachment is the one you delete. Clicking on everything, as some users do, is very unsafe, because an e-mailed virus or worm can send a copy of itself to everyone a user knows, often disguised as something innocent. If you open a file attached to an e-mail, even from someone you know, you are always taking a risk, however small.

Since worms (like KAK) can be concealed in the body of an e-mail, close the preview pane of your e-mail program, because that is what opens the e-mail message (but not attachments) automatically. Also, turn the Windows 98 Scripting Host off:
1. Click on Settings, then Control Panel, then Add/Remove Programs
2. Then click on the Windows Setup tab, then Accessories and if it is checked,
3. Uncheck Windows Scripting Host and Click "OK" to save changes - or click CANCEL if it was not checked.
Note: Web pages that use scripts may not load properly with the Windows Scripting Host disabled, or you may be redirected to alternative pages, that don't use scripts. If you find that inconvenient, you can put the check mark back later (you may need your Windows CD to do that). For Windows 95 and ME, instead of doing the above, locate winscript.exe and rename it, or delete it from the hard disk (after you first copy it to a floppy disk, in case you want to restore it later).

9. **Block Word Macro viruses.** Since only Microsoft Word can open (run) macros that might be embedded in an MS-Word DOC file, those who use Word can enhance their safety by viewing DOC files sent to them by others using a free Viewer, available by download from Microsoft's Web site. Another safety enhancement would be sharing Word files that are saved in Rich Text Format, instead of Word Document format, because files in RTF format do not contain macros, and thus cannot harbor a macro virus. Word 2000 users should also make sure that macro virus protection (under Tools/Macro/Security) is set to High.

Word 97 users should make sure that macro virus protection (under Tools, Options, General) is turned on (checked), and consider password-protecting Normal.dot:
1) Exit Word97, then delete Normal.Dot
2) Start Word, then use Alt-F11 to start the VisualBasic editor
3) Press Ctrl-R to open a window in the upper left corner (if necessary)
4) Click Normal in that window
5) From the Tools menu, select Normal Properties, then Protection
6) Check "Lock project for viewing" and enter a password
7) Click OK, then press Alt-Q to exit the editor
Remember the password, because while this procedure protects Normal.dot from viruses, you will need the password if you want to modify Normal.dot, to record your own macros, for example.

10. **Stop virus hoaxes.**

Did a **genuine computer security expert send you the alert?** If your mother-in-law forwarded a chain letter alert, which came from her dentist, who got it from a podiatrist, who got it from his secretary's daughter, who supposedly received it at college directly from IBM's virus experts.

Does the email offer a link to an **authoritative** details page? Email alerts shouldn't go into detail about a computer virus. Rather, the alert should
summarize the threat and provide a link to a "for more info" page stored on a well-known computer security website. **Beware:** some hoax alerts include generic links to respected websites. The hoaxster wants you to assume the website has important information about the virus. A rule of thumb: the link to more information should take you directly to more information about the threat. If it doesn't, then you should chide the sender for failing to give you accurate information.

Does it urge you to forward the chain letter to everyone you know? Genuine virus alerts won't ask you to participate in a chaotic email distribution scheme. Forward it instead to Vmyths.com (see below) so we can study it.
Information Technology Security
Training Requirements:
A Role- and Performance-Based Model
The National Institute of Standards and Technology was established in 1988 by Congress to “assist industry in the development of technology . . . needed to improve product quality, to modernize manufacturing processes, to ensure product reliability . . . and to facilitate rapid commercialization . . . of products based on new scientific discoveries.”

NIST, originally founded as the National Bureau of Standards in 1901, works to strengthen U.S. industry’s competitiveness; advance science and engineering; and improve public health, safety, and the environment. One of the agency’s basic functions is to develop, maintain, and retain custody of the national standards of measurement, and provide the means and methods for comparing standards used in science, engineering, manufacturing, commerce, industry, and education with the standards adopted or recognized by the Federal Government.

As an agency of the U.S. Commerce Department’s Technology Administration, NIST conducts basic and applied research in the physical sciences and engineering, and develops measurement techniques, test methods, standards, and related services. The Institute does generic and precompetitive work on new and advanced technologies. NIST’s research facilities are located at Gaithersburg, MD 20899, and at Boulder, CO 80303. Major technical operating units and their principal activities are listed below. For more information contact the Publications and Program Inquiries Desk, 301-975-3058.

<table>
<thead>
<tr>
<th>Office of the Director</th>
<th>Physics Laboratory</th>
</tr>
</thead>
<tbody>
<tr>
<td>• National Quality Program</td>
<td>• Electron and Optical Physics</td>
</tr>
<tr>
<td>• International and Academic Affairs</td>
<td>• Atomic Physics</td>
</tr>
<tr>
<td></td>
<td>• Optical Technology</td>
</tr>
<tr>
<td></td>
<td>• Ionizing Radiation</td>
</tr>
<tr>
<td></td>
<td>• Time and Frequency(^1)</td>
</tr>
<tr>
<td></td>
<td>• Quantum Physics(^1)</td>
</tr>
<tr>
<td><strong>Technology Services</strong></td>
<td></td>
</tr>
<tr>
<td>• Standards Services</td>
<td></td>
</tr>
<tr>
<td>• Technology Partnerships</td>
<td></td>
</tr>
<tr>
<td>• Measurement Services</td>
<td></td>
</tr>
<tr>
<td>• Technology Innovation</td>
<td></td>
</tr>
<tr>
<td>• Information Services</td>
<td></td>
</tr>
<tr>
<td><strong>Advanced Technology Program</strong></td>
<td></td>
</tr>
<tr>
<td>• Economic Assessment</td>
<td></td>
</tr>
<tr>
<td>• Information Technology and Applications</td>
<td></td>
</tr>
<tr>
<td>• Chemical and Biomedical Technology</td>
<td></td>
</tr>
<tr>
<td>• Materials and Manufacturing Technology</td>
<td></td>
</tr>
<tr>
<td>• Electronics and Photonics Technology</td>
<td></td>
</tr>
<tr>
<td><strong>Manufacturing Extension Partnership Program</strong></td>
<td></td>
</tr>
<tr>
<td>• Regional Programs</td>
<td></td>
</tr>
<tr>
<td>• National Programs</td>
<td></td>
</tr>
<tr>
<td>• Program Development</td>
<td></td>
</tr>
<tr>
<td><strong>Electronics and Electrical Engineering Laboratory</strong></td>
<td></td>
</tr>
<tr>
<td>• Microelectronics</td>
<td>• Intelligent Processing of Materials</td>
</tr>
<tr>
<td>• Law Enforcement Standards</td>
<td>• Ceramics</td>
</tr>
<tr>
<td>• Electricity</td>
<td>• Materials Reliability(^1)</td>
</tr>
<tr>
<td>• Semiconductor Electronics</td>
<td>• Polymers</td>
</tr>
<tr>
<td>• Electromagnetic Fields(^1)</td>
<td>• Metallurgy</td>
</tr>
<tr>
<td>• Electromagnetic Technology(^1)</td>
<td>• NIST Center for Neutron Research</td>
</tr>
<tr>
<td>• Optoelectronics(^1)</td>
<td></td>
</tr>
<tr>
<td><strong>Chemical Science and Technology Laboratory</strong></td>
<td></td>
</tr>
<tr>
<td>• Biotechnology</td>
<td>• Precision Engineering</td>
</tr>
<tr>
<td>• Physical and Chemical Properties(^2)</td>
<td>• Automated Production Technology</td>
</tr>
<tr>
<td>• Analytical Chemistry</td>
<td>• Intelligent Systems</td>
</tr>
<tr>
<td>• Process Measurements</td>
<td>• Fabrication Technology</td>
</tr>
<tr>
<td>• Surface and Microanalysis Science</td>
<td>• Manufacturing Systems Integration</td>
</tr>
<tr>
<td><strong>Manufacturing Engineering Laboratory</strong></td>
<td></td>
</tr>
<tr>
<td>• Structures</td>
<td>• Structures</td>
</tr>
<tr>
<td>• Building Materials</td>
<td>• Building Environment</td>
</tr>
<tr>
<td>• Building Environment</td>
<td>• Fire Safety Engineering</td>
</tr>
<tr>
<td>• Fire Science</td>
<td>• Fire Science</td>
</tr>
<tr>
<td><strong>Information Technology Laboratory</strong></td>
<td></td>
</tr>
<tr>
<td>• Mathematical and Computational Sciences(^2)</td>
<td></td>
</tr>
<tr>
<td>• Advanced Network Technologies</td>
<td>• Computer Security</td>
</tr>
<tr>
<td>• Computer Security</td>
<td>• Information Access and User Interfaces</td>
</tr>
<tr>
<td>• Information Access and User Interfaces</td>
<td>• High Performance Systems and Services</td>
</tr>
<tr>
<td>• High Performance Systems and Services</td>
<td>• Distributed Computing and Information Services</td>
</tr>
<tr>
<td>• Distributed Computing and Information Services</td>
<td></td>
</tr>
<tr>
<td>• Software Diagnostics and Conformance Testing</td>
<td></td>
</tr>
</tbody>
</table>

\(^1\)At Boulder, CO 80303.
\(^2\)Some elements at Boulder, CO.
Information Technology Security Training Requirements: A Role- and Performance-Based Model

Mark Wilson — Editor
Dorothea E. de Zafra
Sadie I. Pitcher
John D. Tressler
John B. Ippolito

COMPUTER SECURITY

Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-0001

Supersedes Special Publication 500-172

April 1998

U.S. Department of Commerce
William M. Daley, Secretary

Technology Administration
Gary R. Bachula, Acting Under Secretary for Technology

National Institute of Standards and Technology
Raymond G. Kammer, Director
Reports on Computer Systems Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the Nation's measurement and standards infrastructure for information technology. ITL develops tests, test methods, reference data, proof of concept implementations and technical analyses to advance the development and productive use of information technology. ITL's responsibilities include the development of technical, physical, administrative, and management standards and guidelines for the cost-effective security and privacy of sensitive unclassified information in federal computer systems. This Special Publication 800 series reports on ITL's research, guidance, and outreach efforts in computer security, and its collaborative activities with industry, government, and academic organizations.

National Institute of Standards and Technology Special Publication 800-16
CODEN: NSPUE2

U.S. GOVERNMENT PRINTING OFFICE
WASHINGTON: 1998

FOREWORD

In 1997 the General Accounting Office (GAO) identified information technology (IT) security as “a new high-risk area that touches virtually every major aspect of government operations” (report # GAO/HR-97-30). In doing so, GAO went beyond dozens of specific recommendations in its prior reports to identify underlying factors. Several are people factors, not technological factors, e.g., “insufficient awareness and understanding of information security risks among senior agency officials,” “poorly designed and implemented security programs,” “a shortage of personnel with the technical expertise needed to manage controls,” and “limited oversight of agency practices.”

The key to addressing people factors or competencies is awareness, training, and education. Certainly the need for government-wide attention to this area of IT security has never been greater, so issuance of this publication, Information Technology Security Training Requirements: A Role- and Performance-Based Model, (Training Requirements) is especially timely. This document has been designed as a “living handbook” to have the longest useful life possible as the foundation of and structure for “do-able” training by Federal agencies. To meet this objective, the following elements have been included in this document’s design:

- Dates, references, or other items that would quickly outdate the Training Requirements have been excluded. Excluded also are “terms du jour” and items which may be specific to a given agency or Department. Technical jargon changes rapidly—even though the meanings are not significantly different. Thus, to avoid unnecessary outdating, the document uses terminology that is most consistent across Federal agencies and broadest in scope to encompass all information processing, storage, and transmission resources and technologies—for example, “Information Technology.” A glossary of key terms is provided in an appendix.

- An extensible set of knowledges, skills, and abilities (KSAs) structure the Training Requirements and are linked to the document through generic IT Security Body of Knowledge, Topics and Concepts categories as shown in Exhibit 4-4. Thus, new technologies and associated terminology may be added to the KSAs (which are to be maintained in a separate database), and will be tracked forward through the generic IT Security Body of Knowledge, Topics and Concepts categorization to recommended instructional blocks defined in Chapter 4. This linkage precludes a need to continually revise or supersede the key chapter that addresses training criteria with respect to security requirements affected by the ongoing evolution of information technology.

- Finally, the emphasis of the Training Requirements is on training criteria or standards, rather than on specific curricula or content. The training criteria are established according to trainees’ role(s) within their organizations, and are measured by their on-the-job performance. This emphasis on roles and results, rather than on fixed content, gives the Training Requirements flexibility, adaptability, and longevity.
ACKNOWLEDGMENTS

NIST acknowledges the many people who assisted with the development of this document. We thank the members of the Federal Computer Security Program Managers’ Forum and the Federal Information Systems Security Educators’ Association (FISSEA), and in particular, the four members of the FISSEA working group who co-authored the document:

Ms. Dorothea E. de Zafra
Senior Program Analyst and Science Education Program Coordinator
National Institutes of Health
U.S. Department of Health and Human Services

Ms. Sadie I. Pitcher
Information Technology Security Manager (Retired)
U.S. Department of Commerce

Mr. John D. Tressler
Computer Security Officer
Office of the Deputy Chief Information Officer
U.S. Department of Education

Mr. John B. Ippolito
Director, IT Security Services
Allied Technology Group, Inc.

Several colleagues made special contributions to this final product, and the authors gratefully acknowledge their assistance: Ms. Kathie Everhart (NIST) served as the NIST Liaison during the first two years of this document’s development and provided valuable contributions in such areas as the “Basics and Literacy” curriculum; Dr. W. Vic Maconachy (National Security Agency) took a lead role in the initial development of the learning continuum and served as the primary interface with the defense and intelligence communities; Ms. Rudolph (Native Intelligence) provided critical subject matter knowledge, computer graphics skills, and editorial support in the formation of the final product; and finally, Dr. Roger Quane (National Security Agency) provided training evaluation expertise and was the primary author of Chapter 5.

NIST also thanks those who reviewed draft versions of this document. Their comments were significant in shaping the final document.
# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>FOREWORD</td>
<td>iii</td>
</tr>
<tr>
<td>ACKNOWLEDGMENTS</td>
<td>iv</td>
</tr>
<tr>
<td>CHAPTER 1. INTRODUCTION</td>
<td>1</td>
</tr>
<tr>
<td>1.1 Background</td>
<td>3</td>
</tr>
<tr>
<td>1.2 Purpose</td>
<td>4</td>
</tr>
<tr>
<td>1.3 Principles of the New Approach: Results-Based Learning</td>
<td>5</td>
</tr>
<tr>
<td>1.4 Use of this Document</td>
<td>7</td>
</tr>
<tr>
<td>1.5 Document Organization</td>
<td>7</td>
</tr>
<tr>
<td>CHAPTER 2. LEARNING CONTINUUM — MODEL AND OVERVIEW</td>
<td>11</td>
</tr>
<tr>
<td>2.1 Introduction to the Model</td>
<td>13</td>
</tr>
<tr>
<td>2.2 Levels of Learning</td>
<td>15</td>
</tr>
<tr>
<td>2.2.1 Awareness</td>
<td>15</td>
</tr>
<tr>
<td>2.2.2 Training</td>
<td>16</td>
</tr>
<tr>
<td>2.2.3 Education</td>
<td>16</td>
</tr>
<tr>
<td>2.3 Comparative Framework</td>
<td>17</td>
</tr>
<tr>
<td>2.4 Learning Styles and Effective Teaching Methods</td>
<td>19</td>
</tr>
<tr>
<td>2.4.1 Ways of Learning and Implications for Instruction</td>
<td>19</td>
</tr>
<tr>
<td>2.4.2 Additional Considerations for Adult Learning</td>
<td>20</td>
</tr>
<tr>
<td>2.4.3 References</td>
<td>21</td>
</tr>
<tr>
<td>CHAPTER 3. SECURITY BASICS AND LITERACY</td>
<td>23</td>
</tr>
<tr>
<td>3.1 Definition and Purpose</td>
<td>25</td>
</tr>
<tr>
<td>3.2 Basics — Core Set of IT Security Terms and Concepts</td>
<td>26</td>
</tr>
<tr>
<td>3.3 Literacy — Curriculum Framework</td>
<td>32</td>
</tr>
<tr>
<td>CHAPTER 4. TRAINING DEVELOPMENT METHODOLOGY:</td>
<td>41</td>
</tr>
<tr>
<td>ROLE-BASED TRAINING</td>
<td>43</td>
</tr>
<tr>
<td>4.1 Introduction</td>
<td>43</td>
</tr>
<tr>
<td>4.2 IT Security Training Matrix Cells</td>
<td>55</td>
</tr>
<tr>
<td>4.2.1 Training Area: Laws and Regulations</td>
<td>57</td>
</tr>
<tr>
<td>4.2.2 Training Area: Security Program</td>
<td>71</td>
</tr>
<tr>
<td>4.2.3 Training Area: System Life Cycle Security</td>
<td>93</td>
</tr>
</tbody>
</table>
# TABLE OF CONTENTS (Continued)

<table>
<thead>
<tr>
<th>Chapter</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>Evaluating Training Effectiveness</td>
<td>155</td>
</tr>
<tr>
<td>5.1</td>
<td>Value of Evaluation in a Training Program</td>
<td>157</td>
</tr>
<tr>
<td>5.2</td>
<td>Purposes of Training Effectiveness Evaluation</td>
<td>158</td>
</tr>
<tr>
<td>5.3</td>
<td>Development of an Evaluation Plan</td>
<td>158</td>
</tr>
<tr>
<td>5.3.1</td>
<td>Behavioral Objectives</td>
<td>159</td>
</tr>
<tr>
<td>5.3.2</td>
<td>Levels of Evaluation</td>
<td>160</td>
</tr>
<tr>
<td>5.4</td>
<td>Implementation of Evaluation Planning</td>
<td>163</td>
</tr>
<tr>
<td>5.5</td>
<td>Summary</td>
<td>170</td>
</tr>
<tr>
<td>5.6</td>
<td>Chapter References</td>
<td>170</td>
</tr>
<tr>
<td>A</td>
<td>Appendix A — Learning Continuum</td>
<td>A-1</td>
</tr>
<tr>
<td>B</td>
<td>Appendix B — Training Matrix</td>
<td>B-1</td>
</tr>
<tr>
<td>C</td>
<td>Appendix C — Glossary</td>
<td>C-1</td>
</tr>
<tr>
<td>D</td>
<td>Appendix D — Selected Government IT Security References</td>
<td>D-1</td>
</tr>
<tr>
<td>E</td>
<td>Appendix E — Job Function-Training Cross Reference</td>
<td>E-1</td>
</tr>
<tr>
<td>I</td>
<td>Index</td>
<td>I-1</td>
</tr>
</tbody>
</table>
## LIST OF EXHIBITS

<table>
<thead>
<tr>
<th>Exhibit</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Exhibit 1-1</td>
<td>NIST SP 500-172 Training Matrix</td>
<td>4</td>
</tr>
<tr>
<td>Exhibit 1-2</td>
<td>Use of this Document</td>
<td>8</td>
</tr>
<tr>
<td>Exhibit 2-1</td>
<td>IT Security Learning Continuum</td>
<td>13</td>
</tr>
<tr>
<td>Exhibit 2-2</td>
<td>Comparative Framework</td>
<td>18</td>
</tr>
<tr>
<td>Exhibit 3-1</td>
<td>ABC’s of Information Technology Security</td>
<td>27</td>
</tr>
<tr>
<td>Exhibit 3-2</td>
<td>IT Security ABC’s—Terms and Concepts</td>
<td>28</td>
</tr>
<tr>
<td>Exhibit 4-1</td>
<td>IT Security Training Matrix</td>
<td>44</td>
</tr>
<tr>
<td>Exhibit 4-2</td>
<td>Cell Format</td>
<td>45</td>
</tr>
<tr>
<td>Exhibit 4-3</td>
<td>Frequency of Sample Job Function Occurrence</td>
<td>47</td>
</tr>
<tr>
<td>Exhibit 4-4</td>
<td>IT Security Body of Knowledge Topics and Concepts</td>
<td>48</td>
</tr>
<tr>
<td>Exhibit 5-1</td>
<td>Evaluation Objectives</td>
<td>164</td>
</tr>
<tr>
<td>Exhibit 5-2</td>
<td>Sample Questionnaire — Level 1 Evaluation Training Assessment by Student</td>
<td>165</td>
</tr>
<tr>
<td></td>
<td>Sample Questionnaire — Level 3 Evaluation Training Assessment by Supervisor</td>
<td>167</td>
</tr>
<tr>
<td>Exhibit 5-4</td>
<td>Correlation of Evaluation Elements</td>
<td>171</td>
</tr>
</tbody>
</table>
CHAPTER
1
INTRODUCTION
CHAPTER 1. INTRODUCTION

1.1 Background

Federal agencies and organizations cannot protect the integrity, confidentiality, and availability of information in today's highly networked systems environment without ensuring that each person involved understands their roles and responsibilities and is adequately trained to perform them. The human factor is so critical to success that the Computer Security Act of 1987 (Public Law [P.L.] 100-235) required that, “Each agency shall provide for the mandatory periodic training in computer security awareness and accepted computer practices of all employees who are involved with the management, use, or operation of each Federal computer system within or under the supervision of that agency.”

In accordance with P.L. 100-235, the National Institute of Standards and Technology (NIST), working with the U.S. Office of Personnel Management (OPM), was charged with developing and issuing guidelines for Federal computer security training. This requirement was satisfied by NIST's issuance of “Computer Security Training Guidelines” (Special Publication [SP] 500-172) in November 1989. In January 1992, OPM issued a revision to the Federal personnel regulations which made these voluntary guidelines mandatory. This regulation, 5 CFR Part 930, is entitled “Employees Responsible for the Management or Use of Federal Computer Systems” and requires Federal agencies to provide training as set forth in NIST guidelines.

The OPM regulation requires training: for current employees; new employees within 60 days of hire; whenever there is a significant change in the agency's IT security environment or procedures, or when an employee enters a new position which deals with sensitive information; and periodically as refresher training, based on the sensitivity of the information the employee handles. Office of Management and Budget (OMB) Circular A-130, “Management of Federal Information Resources,” Appendix III, “Security of Federal Automated Information Resources,” re-emphasizes these mandatory training requirements. In addition, it requires that prior to being granted access to IT applications and systems, all individuals must receive specialized training focusing on their IT security responsibilities and established system rules.

The NIST guidelines in SP 500-172 provided a framework for determining the training needs of particular categories of employees (including contractors) involved with sensitive but unclassified computer systems. The framework reflected the late 1980's when the IT environment was mainframe oriented. The focal point of SP 500-172 is its Training Matrix, shown on the following page as Exhibit 1-1.
1.2 Purpose

OMB Circular A-130, as revised in 1996, required NIST to update SP 500-172. As a result, this document supersedes SP 500-172 and presents a new conceptual framework for providing IT security training. This framework includes the IT security training requirements appropriate for today’s distributed computing environment and provides flexibility for extension to accommodate future technologies and the related risk management decisions.
1.3 Principles of the New Approach: Results-Based Learning

The learning approach presented in this document is designed on the following principles to facilitate results-based learning.

- **Focuses on job functions, or roles and responsibilities specific to individuals, not job titles, and recognizes that individuals have unique backgrounds, and therefore, different levels of understanding.**

The earlier 500-172 focused on various categories of employees. This new approach recognizes that an individual may have more than one organizational role, and will need IT security training which satisfies the specific responsibilities of each role. In addition, because it is not focused on job titles, this approach facilitates more consistent interpretation of training criteria across organizations.

Everyone needs basic training in IT security concepts and procedures. Beyond the basics, this new approach establishes three distinct levels of IT security training: Beginning, Intermediate, and Advanced. Each level is then linked to roles and responsibilities. Because individuals may perform more than one role within the organization, they may need intermediate or advanced level IT security training in their primary job role, but only the beginning level in a secondary or tertiary role. The new concept facilitates training tailored to individual employee needs and career mobility, and to an organization’s evolving or changing mission and mix of job functions. Thus, the concept of refresher training (traditionally viewed as repetitive learning) gives way to the “just-in-time” learning approach, as an individual’s or organization’s IT security training needs evolve or change.

- **Delineates the differences among awareness, training, and education.**

First, this approach considers awareness programs (which are generally well established in Federal agencies/organizations) as a pre-requisite to IT security training. This document defines the term “IT Security Basics and Literacy,” as the transitional learning activity between “Awareness” and “Training.” IT Security Basics and Literacy comprises relatively generic concepts, terms, and associated learning modules that do not significantly differ among categories of employees or organizations. Thus, this approach eliminates redundancies across audience categories and establishes a baseline of IT security knowledge across government which all employees can reasonably be expected to have as they change jobs and organizations. This baseline is independent of specific IT systems.
Second, the critical differences between “Training” and “Education” are often overlooked. “Education” is clearly identified in this new model as a separate learning level, while recognizing that the education level’s applicability is limited to an organization’s designated IT security specialists. Providing formal education to this group is outside the purview of most Federal agency training programs—with some notable exceptions among national security-related agencies. This document takes the view that education (as distinguished from training) and associated on-the-job experience are essential for IT security specialists to be able to fulfill their roles in an effective manner. The provision of specific criteria for the education level is beyond the scope of NIST’s mandate and, therefore, is beyond the scope of this document.

- **Provides an integrated framework (planning tool) to identify training needs throughout the workforce and ensure that everyone receives appropriate training.**

  The model presented in this document relates job function to required IT security knowledge. This allows managers to identify the training needed to fulfill their IT security responsibilities, to understand the consequences of denying or deferring training, and to plan and schedule training according to organizational priorities.

- **Provides a course development tool.**

  Course developers can readily identify the learning outcomes expected for individuals in various roles with varying responsibilities. This will facilitate the development of IT security course material targeted to the needs of the Federal workforce and will encourage the development of “plug and play” training modules that can be readily customized or adapted to an organization’s needs.

- **Provides a structure for evaluating learning effectiveness.**

  Providing training to individuals does not necessarily ensure that learning has occurred. Learning can best be demonstrated by subsequent on-the-job performance. This document’s learning objectives are designed to be performance-based, rather than content-based, and to provide benchmarks for evaluating learning effectiveness. Further, this document requires evaluation as a component of an organization’s IT security training program and provides an evaluation planning process and a discussion of levels of evaluation.

- **Is extensible.**

  This document is intended to be issued in looseleaf format for extensibility and ease of updating. It is designed to be used as a “living” handbook and reference, with evolving
criteria, exhibits, and appendices that will enable Federal agencies and organizations to ensure that their workforce keeps abreast of changes in information technology and the impact of such changes on the protection of information and systems.

1.4 Use of this Document

The overall goal for use of this document is to facilitate the development or strengthening of a comprehensive, measurable, cost-effective IT security program which supports the missions of the organization and is administered as an integral element of sound IT management and planning. Protecting the value of an organization’s information assets demands no less. This approach allows senior officials to understand where, in what way, and to what extent IT-related job responsibilities include IT security responsibilities, permitting the most cost-effective allocation of limited IT security training resources.

The issuance of this document is not intended to significantly modify Federal agencies’ ongoing IT security awareness programs and activities, or to invalidate their IT security training courses or courseware. Rather, their courses will require comprehensive review and revalidation in accordance with this new performance-based model and requirements. It is expected that agencies and organizations will find training gaps and will need to establish priorities and strategies for filling them. This process cannot be accomplished by a single organization’s IT security program office working alone. Instead, it requires a broad, cross-organizational strategy at the executive level to bring together various functions and organization entities that may not have previously worked together. The perspectives and expertise of training center personnel, course designers, program analysts, IT security specialists, training evaluators, and specialists in many related IT functional areas all are needed to achieve success. To assist in achieving this goal, Exhibit 1-2, on the next page, identifies groups of individuals who will be able to use this guidance document and suggests ways in which they may want to use it.

1.5 Document Organization

This guidance document is organized as follows.

- **Chapter 1, Introduction:** Provides background information citing the statutory and regulatory requirements for IT security training. Establishes the purpose of this document in superseding NIST SP 500-172. Describes the principles of the role- and results-based approach to training taken in this document. Identifies who will be able to use this guidance and suggests ways of using the document.
### Exhibit 1-2
Use of this Document

<table>
<thead>
<tr>
<th>Who Should Use This Document</th>
<th>How This Document Can Be Used</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management — all levels including team leaders, program managers,</td>
<td>• To determine staff training needs</td>
</tr>
<tr>
<td>system managers, and organization leaders</td>
<td>• To prioritize use of training resources</td>
</tr>
<tr>
<td></td>
<td>• To evaluate training effectiveness</td>
</tr>
<tr>
<td>IT Security Specialists</td>
<td>• To identify training courses and training aids that meet established requirements</td>
</tr>
<tr>
<td></td>
<td>• To identify training gaps and needs in the organization’s IT security program</td>
</tr>
<tr>
<td></td>
<td>• To determine the amount of course customization needed</td>
</tr>
<tr>
<td></td>
<td>• To develop a compliance baseline for the organization</td>
</tr>
<tr>
<td>Training Professionals</td>
<td>• To gain an understanding of IT security requirements and the knowledges, skills, and abilities needed to meet those requirements</td>
</tr>
<tr>
<td>• Career Planners/Human Resource Personnel</td>
<td>• To evaluate course quality</td>
</tr>
<tr>
<td>• Training Coordinators/Curriculum Developers</td>
<td>• To assist in obtaining appropriate courses and materials</td>
</tr>
<tr>
<td>• Course Developers</td>
<td>• To develop or customize courses/materials</td>
</tr>
<tr>
<td>• Trainers</td>
<td>• To tailor their teaching approach to achieve the desired behavioral outcomes</td>
</tr>
<tr>
<td>Every Employee</td>
<td>• To identify IT security training needs for their current job assignment and career path</td>
</tr>
</tbody>
</table>
• **Chapter 2, Learning Continuum — Model and Overview:** Introduces a role-based learning model that presents learning as a continuum from awareness through training to education and presents concepts associated with the model. Briefly discusses IT security awareness and education, and explains that detailed treatment of these areas is outside the scope of this document. Provides a comparison highlighting the differences among the three levels of learning and provides a transition to the following chapters, which concentrate on the two training layers of the model, Security Basics and Literacy and Roles and Responsibilities Relative to IT Systems. Discusses learning styles and effective teaching methods, ways of learning and implications for instruction, and presents some additional considerations for adult learning.

• **Chapter 3, IT Security Basics and Literacy:** Presents a core set of generic IT security terms and concepts for all Federal employees as a baseline for further, role-based learning, expands on those basic concepts, and provides a mechanism for students to relate and apply on the job the information learned.

• **Chapter 4, Training Development Methodology: Role-Based Training:** Builds on the Security Basics and Literacy training layer by presenting specific performance-based training requirements and outcomes mapped to job functions. Examines six role categories relative to IT systems—Manage, Acquire, Design and Develop, Implement and Operate, Review and Evaluate, and Use (with a seventh category, “Other” included to provide extensibility). Presents a matrix to relate the categories to three training content categories—Laws and Regulations, Security Program, and System Life Cycle Security. Identifies a set of 12 high-level IT security body of knowledge topics and concepts appropriate to each cell in the matrix from which curriculum content can be constructed. *The training requirements presented here were derived from the IT security program requirements established in Appendix III of OMB Circular A-130.*

• **Chapter 5, Evaluating Training Effectiveness:** Requires evaluation as a component of an organization’s IT security training program. Identifies purposes of evaluation, presents progressive levels of training evaluation, and provides guidance in evaluation planning and implementation.

In addition, this document is supported by several Appendices designed to facilitate its ease of use and to amplify portions of the document which require a more in-depth treatment. These include the following.

• **Appendix A, Information Technology Security Learning Continuum:** Shows a full-page presentation of the Learning Model introduced in Chapter 2.
Appendix B, Information Technology Security Training Matrix: Presents a full-page illustration of how the individual training modules fit together, as used in Chapter 4.

Appendix C, Glossary: Defines key terms used in this document.

Appendix D, Selected Government IT Security References: Provides documentation and sources of material which are related to Federal IT Security Training.

Appendix E, Job Function-Training Cross Reference: Provides a graphical display of the training modules recommended for individuals performing a specific job function.
CHAPTER 2

LEARNING CONTINUUM - MODEL AND OVERVIEW
2.1 Introduction to the Model

The model presented as Exhibit 2-1 is based on the premise that learning is a continuum. Specifically, learning in this context starts with awareness, builds to training, and evolves into education. This model provides the context for understanding and using this document.
The model is role-based. It defines the IT security learning needed as a person assumes different roles within an organization and different responsibilities in relation to IT systems. This document uses the model to identify the knowledges, skills, and abilities an individual needs to perform the IT security responsibilities specific to each of his or her roles in the organization.

The type of learning that individuals need becomes more comprehensive and detailed at the top of the continuum. Thus, beginning at the bottom, all employees need awareness. Training (represented by the two bracketed layers “Security Basics and Literacy” and “Roles and Responsibilities Relative to IT Systems”) is required for individuals whose role in the organization indicates a need for special knowledge of IT security threats, vulnerabilities, and safeguards. The “Education and Experience” layer applies primarily to individuals who have made IT security their profession.

The model illustrates the following concepts:

- “Security Awareness” is explicitly required for ALL employees, whereas “Security Basics and Literacy” is required for those employees, including contractor employees, who are involved in any way with IT systems. In today’s environment this typically means all individuals within the organization.

- The “Security Basics and Literacy” category is a transitional stage between “Awareness” and “Training.” It provides the foundation for subsequent training by providing a universal baseline of key security terms and concepts.

- After “Security Basics and Literacy,” training becomes focused on providing the knowledges, skills, and abilities specific to an individual’s “Roles and Responsibilities Relative to IT Systems.” At this level, training recognizes the differences between beginning, intermediate, and advanced skill requirements.

- The “Education and Experience” level focuses on developing the ability and vision to perform complex multi-disciplinary activities and the skills needed to further the IT security profession and to keep pace with threat and technology changes.

Learning is a continuum in terms of levels of knowledge, but the acquisition or delivery of that knowledge need not proceed sequentially. Given resource constraints, organizations have a responsibility to evaluate against the continuum both the scope of their IT security training needs and the effectiveness of the training provided, to be able to allocate future training resources to derive the greatest value or return on investment.
2.2 Levels of Learning

2.2.1 Awareness

Awareness is not training. The purpose of awareness presentations is simply to focus attention on security. Awareness presentations are intended to allow individuals to recognize IT security concerns and respond accordingly. In awareness activities the learner is a recipient of information, whereas the learner in a training environment has a more active role. Awareness relies on reaching broad audiences with attractive packaging techniques. Training is more formal, having a goal of building knowledge and skills to facilitate job performance.

A few examples of IT security awareness materials/activities include:

- Promotional/speciality trinkets with motivational slogans,
- A security reminder banner on computer screens, which comes up when a user logs on,
- Security awareness video tapes, and
- Posters or flyers.

Effective IT security awareness presentations must be designed with the recognition that people tend to practice a tuning-out process called acclimation. If a stimulus, originally an attention-getter, is used repeatedly, the learner will selectively ignore the stimulus. Thus, awareness presentations must be on-going, creative, and motivational, with the objective of focusing the learner’s attention so that the learning will be incorporated into conscious decision-making. This is called assimilation, a process whereby an individual incorporates new experiences into an existing behavior pattern.

Learning achieved through a single awareness activity tends to be short-term, immediate, and specific. Training takes longer and involves higher-level concepts and skills. For example, if a learning objective is “to facilitate the increased use of effective password protection among employees,” an awareness activity might be the use of reminder stickers for computer keyboards. A training activity might involve computer-based instruction in the use of passwords, parameters, and how to change the passwords for organization systems.

Detailed guidance on IT security awareness is outside the scope of this document. Awareness, as originally defined in 1989 in NIST SP 500-172, “creates the [employee’s] sensitivity to the threats and vulnerabilities of computer systems and the recognition of the need to protect data, information, and the means of processing them.” The fundamental value of IT security awareness programs is that they set the stage for training by bringing about a change in attitudes which change the organizational culture. The cultural change is the realization that IT security is critical because a security failure has potentially adverse consequences for everyone. Therefore, IT security is everyone’s job.
2.2.2 Training

The “Training” level of the learning continuum strives to produce relevant and needed security skills and competency by practitioners of functional specialties other than IT security (e.g., management, systems design and development, acquisition, auditing). The training layers are discussed in detail in Chapters 3 (Security Basics and Literacy) and 4 (Training Development Methodology: Role-Based Training).

2.2.3 Education

The “Education” level integrates all of the security skills and competencies of the various functional specialties into a common body of knowledge, adds a multi-disciplinary study of concepts, issues, and principles (technological and social), and strives to produce IT security specialists and professionals capable of vision and pro-active response.

Historically, “computer security specialists” were practitioners appointed from the ranks of “computer specialists” (or another functional specialty), as if designation alone made those individuals specialists in security. Security responsibilities were often assigned as collateral to the duties of the primary functional specialty.

At best, Federal agencies paid for occasional training courses for their designated Computer Security Officers or specialists; but few agency officials recognized a need to enroll their designees in a formal computer security educational program—or required evidence of qualification or certification as a condition of appointment or collateral designation. IT Security professionalization was not mandated as a component of agency computer security training programs: it was outside the scope of the then-current Federal computer security training guidelines (SP 500-172).

Now, however, the IT Security Specialist/Officer/Program Manager functions have become too technologically and managerially complex to be successfully accomplished—especially on an ancillary or collateral basis—by practitioners lacking a comprehensive set of competencies. Moreover, organization officials, customers, technical personnel, and other stakeholders are creating pressures and demands for creative and dependable solutions to a growing range, number, and severity of security and privacy concerns—solutions which can only be achieved by
a class of professionals with expertise in system and information protection. IT security professionalization is rapidly becoming a “business competency” in the public and private sectors.

IT security professionalization criteria are outside the scope of this document. The training guidance in Chapter 4 can be used and sequenced by agencies on an individualized basis as a cost-effective way to fill gaps in a given practitioner’s knowledge and prepare him/her for formal education that may be needed for credentialing or other demonstrable measures of qualification in IT security.

An IT security professional is one who integrates the principles of the IT security field in a forward-looking manner to keep up with technology trends and their evolving security implications. At the “Training” level of the learning continuum, the specific knowledge and skills acquired may become obsolete as technology changes. The exploratory nature of education differentiates it from training. From this exploratory vantage point, advances in thought and theory make their way into security practices taught in training programs. The educated IT security professional has the comprehensive grasp of the field required to take responsibility for their further learning in an ever-changing environment.

At the advanced level of IT security professionalization, such as that of an IT Security Program Manager, an employee should be able to represent the organization and participate actively and constructively in addressing interagency or cross-cutting issues and concerns. Examples include increasing the effectiveness of assurance techniques; developing security policy models; participating in symposia or workgroups; or contributing to, developing, or managing training programs.

To reach the advanced level of IT security professionalization, completion of formal education in the field is required. With regard to formal education, organizational officials who appoint/supervise IT security specialists should know two important points: first, a concentration or major can be located in any of a number of departments or colleges—from business administration to computer science; and second, regardless of where a concentration or major may be placed in a given university, the program of study should incorporate a well-planned infusion of communications technology, human/behavioral science, mathematics, computer science, engineering, business ethics, and information law.

2.3 Comparative Framework

As illustrated in the learning continuum, “Awareness” constitutes the point-of-entry for all employees into the progression of IT security knowledge levels; the “Training” level, starting with “Security Basics and Literacy,” then builds a wide range of security-related skills needed by employees in several functional area categories; and the “Education” level is the capstone of the learning continuum—creating expertise necessary for IT security specialists and professionals.
Thus, “In a training environment the employee is taught to use specific skills as part of exacting job performance. In an educational context the employee would be encouraged to examine and evaluate not only skills and methods of work but fundamental operating principles and tenets upon which job skills are based....”¹

The distinction among the three levels is not always easy to interpret and apply. Exhibit 2-2, below, illustrates this distinction.

<table>
<thead>
<tr>
<th>Exhibit 2-2</th>
<th>Comparative Framework²</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>AWARENESS</td>
</tr>
<tr>
<td>Level:</td>
<td>Information</td>
</tr>
<tr>
<td>Learning Objective:</td>
<td>Recognition and Retention</td>
</tr>
<tr>
<td>Example Teaching Method:</td>
<td>Media</td>
</tr>
<tr>
<td></td>
<td>- Videos</td>
</tr>
<tr>
<td></td>
<td>- Newsletters</td>
</tr>
<tr>
<td></td>
<td>- Posters</td>
</tr>
<tr>
<td>Test Measure:</td>
<td>True/False Multiple Choice</td>
</tr>
<tr>
<td>Impact Timeframe:</td>
<td>Short-term</td>
</tr>
</tbody>
</table>


2.4 Learning Styles and Effective Teaching Methods

Exhibit 2-2 illustrates learning objectives and examples of teaching methods at each level of the Learning Continuum. This section further develops the role and importance of teaching methods relative to learning for users of this document who may not be training professionals. The Federal workforce is the intended audience for this guidance document, and it is not a single, homogeneous entity. Therefore, no uniform teaching approach, or set of materials, is appropriate. Course developers and trainers will need to select the training materials and approaches that will best address the needs of given audiences in line with an organization’s culture and requirements, as well as with individual student needs as outlined below.

2.4.1 Ways of Learning and Implications for Instruction

Individuals learn in different ways. The learning approach most effective for a particular individual is a function of their preferred learning style, education, and prior experience. While a discussion of learning theory is beyond the scope of this document, it is important for subject matter specialists who may serve as instructors to know that students will not all take in and process information in the same way. Attention to these differences in the instructional process is just as important as is attention to the subject matter itself.

![Chinese Proverb]

"I hear and I forget.  
I see and I remember.  
I do and I understand.”  

— Chinese Proverb

Learning Style: Individuals learn in several ways but each person, as part of their personality, has a preferred or primary learning style. Instruction can positively or negatively affect a student’s performance, depending on whether it is matched, or mismatched, with a student’s preferred learning style. In learning information or concepts, some students will do better through reading (visual learning); others prefer to listen to a lecture (auditory learning); still others need to participate in a discussion (kinesthetic or tactile learning) in order to refine and finally grasp the material. In learning practical skills, some students prefer “how-to” pictures or diagrams (visual learning); others prefer to hear verbal instructions (auditory learning); still others ignore directions and prefer to jump in and figure things out as they go along (kinesthetic or tactile learning).

Content specialists tend to make the mistake of equating teaching to telling. They find out the hard way that students who do not learn best through listening will tune out lectures and learn little. Being aware of learning style differences should motivate instructors to use a variety of teaching approaches. For example, instructors who physically move around the classroom, who
plan silent reading as well as lecturing, who include small group problem-solving, large group debate, brainstorming, blackboard diagraming and other visual aids will have something for everyone and in so doing will eliminate the “yawn factor.” The implications for courseware developers is that there is substantial benefit in using flexible presentation formats (e.g., multimedia, searchable databases, text, graphics, simulations, team teaching, decision trees and interactive learning). A training program as a whole should ideally include a range of delivery approaches. These could include, in addition to classroom instruction and computer-based instruction, such options as manuals and self-paced instruction books, videotapes, interactive workshops with “hands-on” exercises, and one-on-one mentoring/coaching by senior staff.

**Education and prior experience:** Materials developers and trainers should consider the likely education and experience of their target audience and adjust their presentation approach and content accordingly. An individual with an advanced degree will perceive and learn new material in a manner that is different from an individual without a degree but who has extensive on-the-job experience. For example, individuals with more than 15 years of employment (e.g., an older audience) are less likely to be familiar with or comfortable with technology-oriented teaching techniques. However, if the target audience primarily consists of individuals who have recently graduated from college or high school (e.g., a younger audience), then increasing the proportion of material delivered through multimedia or computer-based instruction may be appropriate, as today’s students are generally more experienced with these teaching approaches. The actual job functions of the target audience should also be considered when developing training materials and selecting teaching methodologies. For example, if instruction relating to the IT security countermeasures of a network server is being presented to an audience of system administrators, then a multi-day, hands-on approach might be most effective. If the same material is to be presented to a group of system designers, then a 2-hour lecture may be sufficient.

### 2.4.2 Additional Considerations for Adult Learning

Course developers and trainers should also be aware that adults have well established—not formative—values, beliefs, and opinions. Individuals have individual learning style preferences and adults may have had differing education, varying years of experience, and a wealth of previously learned information which they bring to the learning venue. Adults relate new information and knowledge to previously learned information, experiences, and values—sometimes consciously, sometimes unconsciously—thus, misperception and miscommunication can occur unless instructors make the effort to draw students out. This can be done (at least in a classroom setting) by balancing the presentation of new material with student sharing of relevant experiences. Instructors can help to make connections between various student opinions and ideas, while focusing class effort on integration of the new knowledge or skill with respect to its application.
Team teaching, if that is an option, can leverage individual instructor’s respective skills in this regard. In any case, the involvement of adult students as resources can help overcome potential problems associated with classes composed of workforce students with differing levels of subject-matter knowledge. Otherwise, instructors who rely on giving a lecture of the material risk finding themselves over the heads of beginners, while boring or talking down to students who are at more advanced levels.

Finally, adult students, more so than their younger counterparts, learn best when they perceive the relevance of the knowledge or skill to their current job or to their career advancement. When the instructor is able to emphasize the applicability and practical purpose of the material to be mastered, as distinguished from abstract or conceptual learning, the learning retention rates and the subsequent transference of the new knowledge or skill to the students’ jobs and organizational settings will be enhanced.

2.4.3 References

For further information, the following resources are suggested as a point of departure. This is not an exhaustive listing.

   Cantor, Jeffrey A. Delivering Instruction to Adult Learners. Toronto: Wall & Emerson, 1992.


CHAPTER 3. SECURITY BASICS AND LITERACY

3.1 Definition and Purpose

The Security Basics and Literacy level on the learning continuum is the transition between awareness and training. To draw an analogy with reading literacy, "awareness" is equivalent to reading readiness, whereby the child learns to recognize and memorize the letters of the alphabet. Then, at the transitional level, the child learns to use the alphabet and principles of grammar and sentence structure to read and become literate. The ability to read is the foundation for further, specific learning. So, too, are Security Basics and Literacy the foundation for further specific learning related to one’s role(s) with respect to IT systems.

IT Security literacy must not be confused with the term “computer literacy,” which refers to an individual’s familiarity with a basic set of knowledge needed to use a computer. IT Security literacy refers to an individual’s familiarity with—and ability to apply—a core knowledge set (i.e., “IT security basics”) needed to protect electronic information and systems. Just as computer literacy is a generic foundation, i.e., is not geared to specific technology or application(s), so, too, is security literacy a one-size-fits-all foundation for further learning; it is not geared to any specific system. All individuals who use computer technology or its output products, regardless of their specific job responsibilities, must know IT security basics and be able to apply them.

The next step beyond IT Security Basics and Literacy is to focus individuals’ ongoing learning on their respective job functions and the system(s) they are involved with. That focusing step or stage constitutes the beginning level of specific, role-based IT security training, and is covered in Chapter 4, Training Development Methodology: Role-Based Training. In Chapter 4, “beginning” refers to the beginning of IT security skills training, a logical segue from the knowledge base established here.

The Security Basics and Literacy level has the following learning objectives:

- To ensure that the student knows the “alphabet,” i.e., a core set of key terms and essential concepts which comprises IT security and is essential for the protection of information and systems. (Many of the terms and concepts should have been previously introduced to the learner in an agency’s awareness briefings or activities. In that case, Security Basics and Literacy properly provides reinforcement and structure.)

- To establish the principles for “reading” or “using the alphabet.”

- To promote personal responsibility and positive behavioral change.
To offer a curriculum framework to promote consistency across government.

These objectives are designed to permit a consistent, government-wide approach to ensure that all employees who are involved with IT systems—regardless of agency, organizational unit, job function(s), or specific system(s)—acquire the same, comprehensive literacy in security basics. The value of a consistent training program is the portability of security literacy as employees change jobs and organizations.

3.2 Basics — Core Set of IT Security Terms and Concepts

The body of knowledge associated with IT security is large and growing at an increasing rate, commensurate with today’s rapid technological changes. Regardless of its size and growth rate, certain basic concepts form the foundation of any effective IT security program and environment. These terms and concepts must be learned and applied as the individual proceeds from security awareness to training and then to education.

The core set of IT security terms and concepts is presented in this section as the “ABC’s of Information Technology Security,” 26 items related to the alphabet, as summarized in Exhibit 3-1 on the next page and described briefly in Exhibit 3-2. This memory tool approach aids the learning process while communicating fundamental IT security concepts. It is anticipated that course material developed under this model will build on the memory tool approach to learning.

(Text continues after exhibits, on page 32.)
### Exhibit 3-1
**ABC’s OF INFORMATION TECHNOLOGY SECURITY**

| **A** | Assets - Something of value requiring protection (hardware, software, data, reputation) |
| **B** | Backup - The three most important safeguards - backup, backup, backup |
| **C** | Countermeasures and Controls - Prevent, detect, and recover from security incidents |
| **D** | DAA and Other Officials - Manage and accept risk and authorize the system to operate |
| **E** | Ethics - The body of rules that governs an individual’s behavior. |
| **F** | Firewalls and Separation of Duties - Minimize the potential for “incident encroachment” |
| **G** | Goals - Confidentiality, Integrity, and Availability (CIA) |
| **H** | Hackers/Crackers - Intruders who are threats to any system |
| **I** | Individual Accountability/Responsibility - Individuals responsible for their own actions |
| **J** | Job Description/Job Function - Defines the individual’s roles within the organization |
| **K** | Keys to Incident Prevention - Awareness, compliance, common sense |
| **L** | Laws and Regulations - Establish basic control/security objectives |
| **M** | Model Framework - Relates training needs to roles and responsibilities |
| **N** | Need to Know - Limits access to data, sets objective for ongoing learning |
| **O** | Ownership - Establishes responsibility/accountability for asset protection |
| **P** | Policies and Procedures - What to accomplish and how to accomplish it |
| **Q** | Quality Assurance/Quality Control - Ensure the integrity of the process |
| **R** | Risk Management - Balances potential adverse impact against safeguard cost |
| **S** | Security Training - The best return on investment of any security safeguard |
| **T** | Threats - Are always present, and generally occur when least expected |
| **U** | Unique Identifiers - Provide for individual accountability and facilitate access control |
| **V** | Vulnerabilities - Security weaknesses through which threats impact the system |
| **W** | Waste, Fraud, and Abuse - The three primary impacts of a security incident |
| **X** | exXpect the uneXpected - Don’t assume that because something hasn’t happened, it won’t |
| **Y** | You - Your actions/inactions are critical to maintaining an effective security environment |
| **Z** | Zoning/Compartmentalization - Establish security layers and minimize incident impact |
Exhibit 3-2
IT Security ABC’s — Terms and Concepts

- **Assets** — Assets are something of value that requires protection. The value of an asset may be monetary or non-monetary. For example, a computer system clearly has a monetary value that may be expressed in terms of its cost of acquisition or replacement. Data, however, is an asset that may have a monetary value (the cost to acquire), a non-monetary value (loss of public confidence regarding data accuracy), or both.

- **Backup** — Backup for data and/or processes are critical safeguards in any IT security environment. The concept of backup includes creation and testing of disaster recovery and continuity of operations plans as well as preparation of copies of data files that are stored “out of harm’s way.”

- **Countermeasures and Controls** — Countermeasures, controls, and safeguards are terms that are often used synonymously. They refer to the procedures and techniques used to prevent the occurrence of a security incident, detect when an incident is occurring or has occurred, and provide the capability to respond to or recover from a security incident. A safeguard may be a password for a user identifier, a backup plan that provides for offsite storage of copies of critical files, audit trails that allow association of specific actions to individuals, or any of a number of other technical or procedural techniques. Basically, a safeguard is intended to protect the assets and availability of IT systems.

- **DAA and Other Officials** — Individuals are responsible for allocating resources. Resources may be allocated to address IT security issues or any of a number of other competing organizational needs. The individual who has such authority for a specific IT system may be termed a Designated Accrediting Authority (DAA), Approving Authority, Authorizing Official, Recommending Official, or other titles specific to an organization. Whatever the title, the individual who has the authority to allocate resources is also responsible for balancing risks and costs and accepting any residual risks in making those decisions. The accrediting authorities are often helped in these decisions by certifying authorities who provide assessments of the technical adequacy of the current security environment and recommendations for resolving deficiencies or weaknesses.

- **Ethics** — the body of rules that governs an individual’s behavior. It is a product of that individual’s life experiences and forms a basis for deciding what is right and wrong when making decisions. In today’s environment, ethics are, unfortunately, situational (i.e., an individual’s definition of what is right and wrong changes depending on the nature of a particular situation). For example, an individual may believe that it is wrong to break into someone’s house, but does not think that it is wrong to break into someone’s computer system.
Exhibit 3-2
IT Security ABC’s — Terms and Concepts (Continued)

- **Firewalls and Separation of Duties** — Firewalls and separation of duties have similar structures and complementary objectives: a firewall is a technical safeguard that provides separation between activities, systems, or system components so that a security failure or weakness in one is contained and has no impact on other activities or systems (e.g., enforcing separation of the Internet from a Local Area Network). Separation of duties similarly provides separation, but its objective is to ensure that no single individual (acting alone) can compromise an application. In both cases, procedural and technical safeguards are used to enforce a basic security policy that high risk activities should be segregated from low risk activities and that one person should not be able to compromise a system.

- **Goals** — The goals of an IT security program can be summarized in three words: *confidentiality* - data must be protected against unauthorized disclosure; *integrity* - IT systems must not permit processes or data to be changed without authorization; and *availability* - authorized access to IT systems must be assured.

- **Hackers/Crackers** — The term “hacker” was originally coined to apply to individuals who focused on learning all they could about IT, often to the exclusion of many other facets of life (including sleeping and eating). A “cracker” is any individual who uses advanced knowledge of networks or the Internet to compromise network security. Typically, when the traditional hacker compromised the security of an IT system, the objective was academic (i.e., a learning exercise), and any resulting damage or destruction was unintentional. Currently, the term hacker is being more widely used to describe any individual who attempts to compromise the security of an IT system, especially those whose intention is to cause disruption or obtain unauthorized access to data. Hacker/cracker activity generally gets high press coverage even though more mundane security incidents caused by unintentional actions of authorized users tend to cause greater disruption and loss.

- **Individual Accountability/Responsibility** — A basic tenet of IT security is that individuals must be accountable for their actions. If this is not followed and enforced, it is not possible to successfully prosecute those who intentionally damage or disrupt systems, or to train those whose actions have unintended adverse effects. The concept of individual accountability drives the need for many security safeguards such as user identifiers, audit trails, and access authorization rules.

- **Job Description/Job Function** — To provide individuals with the training necessary to do their job, and to establish appropriate safeguards to enforce individual accountability, it is necessary to know what functions an individual is authorized to perform (i.e., their role(s) within the organization). Some times this is accomplished using formalized/written job descriptions. In other situations, such assessments are based on analysis of the functions performed.
### Exhibit 3-2
**IT Security ABC’s — Terms and Concepts** (Continued)

- **Keys to Incident Prevention** — Many IT security incidents are preventable if individuals incorporate three basic concepts into their day-to-day activities: one, awareness - individuals should be aware of the value of the assets they use to do their job and the nature of associated threats and vulnerabilities; two, compliance - individuals should comply with established safeguards (e.g., scanning diskettes, changing passwords, performing backups); and three, common sense - if something appears too good to be true, it generally is.

- **Laws and Regulations** — Congress has enacted a number of laws (e.g., Privacy Act, Computer Security Act, Computer Fraud and Abuse Act) that establish the basic policy structure for IT security in the Federal government. These laws have been augmented with regulations and guidance regarding their applicability to IT systems. Private industry generally grounds its security policies on the impact on profitability and potential risk of lawsuits, as there are few specific legal requirements. The commonality between Federal and private IT security programs demonstrates that the objectives are the same whether the impetus was a law or the bottom line.

- **Model Framework** — This document presents a model framework for IT security training. The model framework describes individual training needs relative to job function or role within the organization. The model recognizes that an individual’s need for IT security training will change, both in scope and depth, relative to their organizational responsibilities.

- **Need to Know** — Need to Know is addressed from two perspectives: first, a need for access to information to do a job; and second, need to know as a driver for continued learning. In the first case, access to information and processes should be restricted to that which the individual requires to do their job. This approach minimizes the potential for unauthorized activities, and maximizes the potential that the individual knows and understands the nature of the threats and vulnerabilities associated with their use or maintenance of an IT system; and second, given the rate of technological change, individuals need to know the characteristics of those technologies so they may be better able to address specific vulnerabilities.

- **Ownership** — Responsibility for the security of an IT system or asset must be assigned to a single, identifiable entity, and to a single, senior official within that entity. This provides for accountability for security failures and establishment of the chain of command that authorizes access to and use of system assets. This concept of individual responsibility and authority is generally termed ownership or stewardship. The ownership of an asset (particularly data) is generally retained, even when that asset is transferred to another organization. For example, tax data shared with other Federal and state agencies by the Internal Revenue Service must be secured in accordance with the Internal Revenue Code.
Policies and Procedures — IT security safeguards are intended to achieve specific control objectives. These objectives are contained within security policies that should be tailored to the needs of each IT system. Procedures define the technical and procedural safeguards that have been implemented to enforce the specified policies. IT security procedures may be documented in a security plan.

Quality Assurance/Quality Control — Quality Assurance and Quality Control are two processes that are used to ensure the consistency and integrity of security safeguards. Specifically, these processes are intended to ensure that security countermeasures perform as specified, under all workload and operating conditions.

Risk Management — Risk management is the process whereby the threats, vulnerabilities, and potential impacts from security incidents are evaluated against the cost of safeguard implementation. The objective of Risk Management is to ensure that all IT assets are afforded reasonable protection against waste, fraud, abuse, and disruption of operations. Risk Management is growing in importance as the scope of potential threats is growing while available resources are declining.

Security Training — Security training is the sum of the processes used to impart the body of knowledge associated with IT security to those who use, maintain, develop, or manage IT systems. A well trained staff can often compensate for weak technical and procedural safeguards. Security training has been demonstrated to have the greatest return on investment of any technical or procedural IT security safeguard.

Threats — Threats are actions or events (intentional or unintentional) which, if realized, will result in waste, fraud, abuse, or disruption of operations. Threats are always present, and the rate of threat occurrence cannot be controlled. IT security safeguards, therefore, must be designed to prevent or minimize any impact on the affected IT system.

Unique Identifiers — A unique identifier is a code or set of codes that provide a positive association between authorities and actions to individuals. Safeguards must be in place to ensure that an identifier is used only by the individual to whom it is assigned.

Vulnerabilities — Vulnerabilities are weaknesses in an IT system’s security environment. Threats may exploit or act through a vulnerability to adversely affect the IT system. Safeguards are used to mitigate or eliminate vulnerabilities.

Waste, Fraud, and Abuse — Waste, fraud, and abuse are potential adverse impacts that may result from a breakdown in IT security. Waste, fraud, and abuse are specifically identified as potential impacts in government-wide policy.
Exhibit 3-2

IT Security ABC’s — Terms and Concepts  (Continued)

- **eXpect the uneXpected** — IT security safeguards target unauthorized actions. Unauthorized actions (acts by individuals or Acts-of-God) can take many forms and can occur at any time. Thus, security safeguards should be sufficiently flexible to identify and respond to any activity that deviates from a pre-defined set of acceptable actions.

- **You** — You are responsible and will be held accountable for your actions relative to an IT system or its associated data. You can strengthen or weaken an IT security environment by your actions or inactions. For example, you can strengthen an IT environment by changing passwords at appropriate intervals and weaken it by failing to do so.

- **Zoning/Compartmenting** — Zoning/Compartmenting is a concept whereby an application is segmented into independent security environments. A breach of security would require a security failure in two or more zones/compartments before the application is compromised. This layered approach to security can be applied within physical or technical environments associated with an IT system.

### 3.3 Literacy — Curriculum Framework

The literacy level is the first solid step of the IT security training level, where the knowledge obtained through training can be directly related to the individual’s role in his or her specific organization. Although the curriculum framework, presented below, provides a generic outline for material to be included in literacy training throughout government, it is imperative that the instructor relate the actual course content to the organization’s unique culture and mission requirements. Emphasis placed on the specific topics may vary by student audience or organization needs. The curriculum framework was developed to present topics and concepts in a logical order, based on IT system planning and life cycle stages, but may be presented in any order. Literacy training may also be divided into more than one session. Regardless of the training method or structure used, it is expected that the actual literacy training, including all topics and concepts in the curriculum framework, can be completed within an 8-hour time frame. This is because, at the literacy level, the material should be presented as an introduction of the concepts and topics only.

There are a variety of suitable approaches for teaching this subject matter. One of the most effective is to encourage participation by the students in interactive discussions on how the various concepts relate to their particular organization or roles. This approach allows the students to understand the significance of IT security principles and procedures to their organization, and to begin finding ways of applying this new knowledge in their work environment.
The following curriculum framework incorporates and expands on the basic concepts introduced in the ABC’s, introduces a set of generic topics and concepts which have been identified as the foundation for IT security training, and provides a mechanism for students to relate and apply the information learned on the job. In Chapter 4, a methodology for development of role-based training, based on an expanded version of these same (generic) topics and concepts, is presented to provide for the in-depth training requirements of individuals who have been assigned specific IT security related responsibilities.

1. Laws and Regulations

Subjects to include:

- Federal IT security laws, regulations, standards and guidelines
- Organization specific policies and procedures
- Role of Federal government-wide and organization specific laws, regulations, policies, guidelines, standards and procedures in protecting the organization’s IT resources
  - Tangible and intangible IT resources (assets)
- Current and emerging social issues that can affect IT assets
- Laws and regulations related to social issues affecting security issues
- Effect of social issues on accomplishment of organizations mission(s)
  - Social conflicts with the Freedom of Information Act
  - Public concern for protection of personal information
- Legal and liability issues
  - Laws concerning copyrighted software
  - Organization policies concerning copyrighted software
  - Laws concerning privacy of personal information
  - Organization policies concerning privacy of personal information
  - Mission related laws and regulations
  - Effects of laws, regulations or policies on the selection of security controls

Includes basic IT security concepts introduced in the following ABC’s:

- L - Laws and Regulations
- P - Policies and Procedures

2. The Organization and IT Security

Subjects to include:

- Organization mission(s)
- How information technology supports the mission(s)
- Reliance on IT systems for mission accomplishment
- IT security programs protect against violations of laws and regulations
- Purpose and elements of organizational IT security programs
• Difference between organization level and system level IT security programs
• Changing IT security issues and requirements
• System ownership and its importance from a user or client perspective
• Information ownership and its importance from a user or client perspective
• Identification of IT security program and system level points of contacts

Includes basic IT security concepts introduced in the following ABC’s:

A - Assets
G - Goals
O - Ownership

3. System Interconnection and Information Sharing

Subjects to include:

• Increased vulnerabilities of interconnected systems and shared data
• Responsibilities of system or information owner organizations if systems have external users or clients
• Responsibility of users or clients for notifying system owners of security requirements
• Sharing information on system controls with internal and external users and clients
• Formal agreements between systems for mutual protection of shared data and resources
  • User rules of behavior and individual accountability in interconnected systems
  • System rules of behavior and technical controls based on most stringent protection requirements
• Electronic mail security concerns
• Electronic commerce
  • Electronic Fund Transfer
  • Electronic Data Interchange
  • Digital/electronic signatures
• Monitoring user activities

Includes basic IT security concepts introduced in the following ABC’s:

A - Assets
C - Countermeasures and Controls
E - Ethics
H - Hackers/Crackers
I - Individual Accountability/Responsibility
T - Threats
V - Vulnerabilities
W - Waste, Fraud, and Abuse
X - eXpect the uneXpected
Y - You
4. Sensitivity

Subjects to include:

- Categorization of system sensitivity
  - Criticality
  - Unauthorized use
  - Reliability
- Categorization of information sensitivity
  - Sensitive information in general
    - Types of sensitive information
    - Aggregation of information
  - Organization’s sensitive information
    - Need to know
    - Authorized access
    - Unauthorized disclosure
- IT asset protection requirements
- The organization’s need for confidentiality of its information
  - Adverse consequences of unauthorized information disclosure
- The organization’s need for integrity of its information
  - Corruption of information
    - Accidental
    - Intentional
  - Adverse consequences if public or other users do not trust integrity and reliability of information
- The organization’s need for availability of its information and IT systems
  - Adverse consequences of system or information unavailability
  - Public dependance on information
  - Internal or external user’s dependence on information

Includes basic IT security concepts introduced in the following ABC’s:

- G - Goals
- N - Need to Know

5. Risk Management

Subjects to include:

- Managing risk
  - Threats
  - Vulnerabilities
  - Risk
• Relationships between threats, vulnerabilities, risks
• Threats from “authorized system users”
• Increased threats and vulnerabilities from connection to external systems and networks
  • “Hacker” threats
  • Malicious software programs and virus threats
• Types of security controls (safeguards, countermeasures)
  • Management controls
  • Acquisition/development/installation/implementation controls
  • Operational controls
  • Security awareness and training controls
  • Technical controls
• How different categories of controls work together
• Examples of security controls for:
  • Confidentiality protection
  • Availability protection
  • Integrity protection
• Added security controls for connecting external systems and networks
• Protecting assets through IT security awareness and training programs
• Contingency-disaster recovery planning
  • Importance of plan to deal with unexpected problems
  • Importance of testing plan and applying lessons learned
• “Acceptable levels of risk” vs. “absolute protection from risk”
• “Adequate” and “appropriate” controls
  • Unique protection requirements of IT systems and information
  • Severity, probability, and extent of potential harm
  • Cost effective/cost benefits
  • Reduction of risk vs. elimination of risk
• Working together with other security disciplines
• Importance of internal and external audits, reviews, and evaluations in security decisions

Includes basic IT security concepts introduced in the following ABC’s:

C - Countermeasures and Controls
R - Risk Management
S - Security Training

6. Management Controls

Subjects to include:

• System/application-specific policies and procedures
• Standard operating procedures
Information Technology Security Training Requirements

- Personnel security
  - Background investigations/security clearances
  - Roles and responsibilities
  - Separation of duties
  - Role-based access controls
- System rules of behavior contribute to an effective security environment
  - Organization-specific user rules
  - System-specific user rules
    - Assignment and limitation of system privileges
    - Intellectual property/Copyright issues
    - Remote access and work at home issues
    - Official vs. unofficial system use
    - Individual accountability
    - Sanctions or penalties for violations
- Individual accountability contributes to system and information quality
  - Individual acceptance of responsibilities
  - Signed individual accountability agreements
- IT security awareness and training
  - Determining IT security training requirements for individuals
  - Effect of IT security awareness and training programs on personal responsibility and positive behavioral changes
    - “Computer ethics”
  - System-specific user IT security training
- User responsibilities for inappropriate actions of others

Includes basic IT security concepts introduced in the following ABC’s:

E - Ethics
I - Individual Accountability/Responsibility
J - Job Description/Job Function
M - Model Framework
P - Policies and Procedures
S - Security Training
Y - You

7. Acquisition/Development/Installation/Implementation Controls

Subjects to include:

- System life cycle stages and functions
- IT security requirements in system life cycle stages
  - Initiation stage
  - Development stage
• Test and evaluation stage
• Implementation stage
• Operations stage
• Termination stage
• Formal system security plan for management of a system
  • Identification of system mission, purpose and assets
  • Definition of system protection needs
  • Identification of responsible people
  • Identification of system security controls in-place or planned and milestone dates for implementation of planned controls
• Relationship of configuration and change management programs to IT security goals
• Testing system security controls synergistically and certification
• Senior manager approval (accredit) an IT system for operation

Includes basic IT security concepts introduced in the following ABC’s:

D - DAA and Other Officials
G - Goals
O - Ownership

8. Operational Controls

Subjects to include:

• Physical and environmental protection
  • Physical access controls
  • Intrusion detection
  • Fire/water/moisture/heat/electrical maintenance
  • Mobile and portable systems
• Marking, handling, shipping, storing, cleaning, and clearing
• Contingency planning
  • Importance of developing and testing contingency/disaster recovery plans
  • Importance of users providing accurate information about processing needs, allowable down time and applications that can wait
  • Responsibility for backup copies of data files and software programs
  • Simple user contingency planning steps

Includes basic IT security concepts introduced in the following ABC’s:

B - Backup
Z - Zoning/Compartmentalization
9. Technical Controls

Subjects to include:

- How technical (role-based access) controls support management (security rules) controls
  - User identification and passwords/tokens
  - User role-based access privileges
  - Public access controls
- How system controls can allow positive association of actions to individuals
  - Audit trails
  - System monitoring
- Recognizing attacks by hackers, authorized or unauthorized users
  - Effects of hacker attack on authorized users
  - Unauthorized use or actions by authorized users
  - Reporting incidents
- User actions to prevent damage from malicious software or computer virus attacks
  - Organization specific procedures for reporting virus incidents
  - Technical support and help from security incident response teams
  - Software products to scan, detect and remove computer viruses
- Role of cryptography in protecting information

Includes basic IT security concepts introduced in the following ABC’s:

- F - Firewalls and Separation of Duties
- H - Hackers/Crackers
- I - Individual Accountability/Responsibility
- J - Job Description/Job Function
- K - Keys to Incident Prevention
- Q - Quality Assurance/Quality Control
- U - Unique Identifiers
- V - Vulnerabilities
- Z - Zoning/Compartmentalization
CHAPTER 4

TRAINING DEVELOPMENT METHODOLOGY:
ROLE-BASED TRAINING
CHAPTER 4. TRAINING DEVELOPMENT METHODOLOGY:
ROLE-BASED TRAINING

4.1 Introduction

The Learning Continuum presented in Chapter 2 shows the relationship among Awareness, Security Basics and Literacy, Training, and Education. The Continuum demonstrates that Awareness and Security Basics and Literacy form the baseline which is required for all individuals involved with the management, development, maintenance, and/or use of IT systems. It also demonstrates that Training and Education are to be provided selectively, based on individual responsibilities and needs. Specifically, Training is to be provided to individuals based on their particular job functions. Education is intended for designated IT security specialists in addition to role-based training. This chapter establishes a model and requirements for the Roles and Responsibilities Relative to IT Systems layer of the Learning Continuum.

Over time, individuals acquire different roles relative to the use of IT within an organization, or as they make a career move to a different organization. Sometimes they will be users of applications; in other instances they may be involved in developing a new system; and in some situations they may serve on a source selection board to evaluate vendor proposals for IT systems. An individual’s need for IT security training changes as their roles change. This is recognized within the Learning Continuum by segmenting the Training level shown above into six functional specialities which represent categories of generic organizational roles: Manage, Acquire, Design and Develop, Implement and Operate, Review and Evaluate, and Use. A seventh category, “Other,” is a place holder, to allow the matrix to be updated to accommodate any additional functional roles identified in the future.

This chapter examines the six role categories relative to three fundamental training content categories:

- Laws and Regulations—the types of knowledge, skills, and abilities (KSAs) relative to the laws and regulations pertaining to information and asset protection that govern the management and use of IT within the Federal Government. These include government-wide requirements such as the Computer Security Act of 1987, policy promulgated by the Office of Management and Budget, standards and guidance disseminated by NIST, as well as policies and procedures specific to a Department or agency;

- Security Program—KSAs relative to the establishment, implementation, and monitoring of an IT Security Program within an organization; and
Information Technology Security Training Requirements

- System Life Cycle Security—KSAs relative to the nature of IT security needed throughout each phase of a given system’s life cycle. In this instance, a six-phased system life cycle model was used (Initiation, Development, Test and Evaluation, Implementation, Operations, and Termination).

Combining the six role categories and the three training areas (with a fourth area, “Other,” added as a place holder for future use) yields the following Information Technology Security Training Matrix, Exhibit 4-1, shown below. This matrix is, in effect, a “pull-down menu” of the Training level in the Learning Continuum.

### Exhibit 4-1
IT Security Training Matrix

<table>
<thead>
<tr>
<th>TRAINING AREAS</th>
<th>FUNCTIONAL SPECIALTIES</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>A MANAGE</td>
</tr>
<tr>
<td>1 LAWS &amp; REGULATIONS</td>
<td>1A</td>
</tr>
<tr>
<td>2 SECURITY PROGRAM</td>
<td></td>
</tr>
<tr>
<td>2.1 PLANNING</td>
<td>2.1A</td>
</tr>
<tr>
<td>2.2 MANAGEMENT</td>
<td>2.2A</td>
</tr>
<tr>
<td>3 SYSTEM LIFE CYCLE SECURITY</td>
<td></td>
</tr>
<tr>
<td>3.1 INITIATION</td>
<td>3.1A</td>
</tr>
<tr>
<td>3.2 DEVELOPMENT</td>
<td>3.2A</td>
</tr>
<tr>
<td>3.3 TEST &amp; EVALUATION</td>
<td></td>
</tr>
<tr>
<td>3.4 IMPLEMENTATION</td>
<td>3.4A</td>
</tr>
<tr>
<td>3.5 OPERATIONS</td>
<td>3.5A</td>
</tr>
<tr>
<td>3.6 TERMINATION</td>
<td>3.6A</td>
</tr>
<tr>
<td>4 OTHER</td>
<td></td>
</tr>
</tbody>
</table>

This chapter presents the training requirements for each of the 46 cells, i.e., 1A through 3.6E. (Bricked cells - particularly 3.1D, 3.3A, 3.3B, 3.6B, and 3.6C - are place holders, or cells that may be used later.) This approach will enable course developers to create a block or module of instructional material relative to the requirements defined in a specific cell with confidence that it will complement and augment training material developed for the other cells. Further, individuals or supervisors will be able to select that training needed to satisfy an individual’s organizational role at a specific point in time, with assurance that such training will contribute to his or her career progression, or to other assigned duties. Finally, trainers will have the flexibility to combine modules (horizontally or vertically) into a comprehensive IT security course or to
insert one or more of the security modules into a training course for one of the functional specialties, such as management, acquisitions, or auditing.

Each cell of the IT Security Training Matrix is detailed in a one-page table, which has the format of the table shown in Exhibit 4-2. Explanation of the cell contents follows:

- **Title Block** — Labels the cell within the matrix and identifies the specific Training Area and Functional Specialty (Role) addressed.
- **Definition** — Defines the training content area addressed.
- **Behavioral Outcome** — Describes what an individual who has completed the specific training module is expected to be able to accomplish in terms of IT security-related job performance.
- **Knowledge Levels** — Provides verbs that describe actions an individual should be capable of performing on the job after completion of the training associated with the cell. The verbs are identified for three training levels: Beginning, Intermediate, and Advanced.

### Exhibit 4-2
#### Cell Format

<table>
<thead>
<tr>
<th>Training Area: Function</th>
<th>Training Area: Functional Specialty:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Definition —</td>
<td></td>
</tr>
<tr>
<td>Behavioral Outcome —</td>
<td></td>
</tr>
<tr>
<td>Knowledge Levels —</td>
<td>1. Beginning —</td>
</tr>
<tr>
<td></td>
<td>2. Intermediate —</td>
</tr>
<tr>
<td></td>
<td>3. Advanced —</td>
</tr>
<tr>
<td>Sample Learning Objectives —</td>
<td>1. Beginning —</td>
</tr>
<tr>
<td></td>
<td>2. Intermediate —</td>
</tr>
<tr>
<td></td>
<td>3. Advanced —</td>
</tr>
<tr>
<td>Sample Job Functions —</td>
<td>•</td>
</tr>
<tr>
<td></td>
<td>•</td>
</tr>
</tbody>
</table>

**IT SECURITY BODY OF KNOWLEDGE TOPICS AND CONCEPTS**

- •
- •
- •

For the content of the numbered topics and concepts above, refer to Exhibit 4-5.
Information Technology Security Training Requirements

- **Sample Learning Objectives** — Links the verbs from the “Knowledge Levels” section to the “Behavioral Outcomes” by providing examples of the activities an individual should be capable of doing after successful completion of training associated with the cell. Again, the Learning Objectives recognize that training must be provided at Beginning, Intermediate, and Advanced levels. For some of the cells, there will not be three distinct levels (i.e., there may be only two levels or even one). In these instances, there is no clear distinction between performance objectives that allows separation into Beginning, Intermediate, and Advanced levels. (Note: Beginning, Intermediate, and Advanced refer to levels of IT security responsibility associated with the functional area, not to levels of the functional area as such. For example, an experienced (Advanced level) IT system developer could be taking entry-level (Beginning) training in the IT security responsibilities associated with the system development function.)

The purpose of the Beginning Level is to focus the generic understanding of IT security, which the individual will have acquired from Security Basics and Literacy (per Chapter 3), on their job requirements.

- **Sample Job Functions** — Presents sample position titles or job functions of individuals who would be expected to obtain the training for a particular cell. Individuals designated as IT Security specialists need to be acquainted with the training content in all cells, whether or not they themselves need training in a specific programmatic role (e.g., responsibility for selecting a back-up site for a specific IT system). An aggregate of 26 Sample Job Functions for all cells is presented as Exhibit 4-3, together with the number of cells in which each occurs. It is not intended to be an exhaustive list of all possible job functions. Appendix E, Job Function-Training Cross Reference, contains tables that show the recommended training modules (cells) for each of these 26 job functions.

- **IT Security Body of Knowledge Topics and Concepts** — This block (on the back of the page for each cell), provides suggested topics and concepts which pertain to the particular cell or training module that will increase the knowledge, skills, and abilities of the student. The numbers on the back of the cell page refer to Exhibit 4-4, which presents twelve high-level topics and concepts intended to incorporate the overall body of knowledge required for training in IT security. Each of these topics and concepts is then broken down into more specific subjects that should be included in the training for that topic. By identifying the twelve topics and concepts at a high level, they become general and flexible categories under which more specific topics or subjects can be added or removed to keep up with evolving technology, laws, regulations, policies, or guidance.

To customize the training in a cell, topics and detailed subjects may be presented at different depths to accomplish the desired learning objective level (i.e., Beginning, Intermediate, and Advanced). For example, if an individual has no acquisition responsibilities and therefore, no need for in-depth training in acquisition, that topic might be introduced, but not explained in depth. Thus, the student would become familiar with the associated IT security considerations, but would not learn how to write...
detailed IT security requirements for a statement of work. In addition, the content may be modified for specific organization or system reasons. The listed topics and concepts are not intended to be absolute, and creators of the actual training courses will be expected to review the suggested topics for each cell and revise them as appropriate.

<table>
<thead>
<tr>
<th>No. of Cells</th>
<th>Exhibit 4-3 Frequency of Sample Job Function Occurrence</th>
</tr>
</thead>
<tbody>
<tr>
<td>46</td>
<td>IT Security Officer/Manager*</td>
</tr>
<tr>
<td>18</td>
<td>System Owner</td>
</tr>
<tr>
<td>16</td>
<td>Information Resources Manager</td>
</tr>
<tr>
<td>15</td>
<td>Program Manager</td>
</tr>
<tr>
<td>11</td>
<td>Auditor, Internal</td>
</tr>
<tr>
<td>10</td>
<td>Network Administrator</td>
</tr>
<tr>
<td>10</td>
<td>System Administrator</td>
</tr>
<tr>
<td>10</td>
<td>System Designer/Developer</td>
</tr>
<tr>
<td>9</td>
<td>Auditor, External</td>
</tr>
<tr>
<td>8</td>
<td>Contracting Officer’s Technical Representative (COTR)</td>
</tr>
<tr>
<td>8</td>
<td>Programmer/Systems Analyst</td>
</tr>
<tr>
<td>8</td>
<td>Systems Operations Personnel</td>
</tr>
<tr>
<td>8</td>
<td>Information Resources Management Official, Senior</td>
</tr>
<tr>
<td>7</td>
<td>Chief Information Officer</td>
</tr>
<tr>
<td>7</td>
<td>Database Administrator</td>
</tr>
<tr>
<td>7</td>
<td>Data Center Manager</td>
</tr>
<tr>
<td>6</td>
<td>Certification Reviewer</td>
</tr>
<tr>
<td>6</td>
<td>Contracting Officer</td>
</tr>
<tr>
<td>6</td>
<td>User</td>
</tr>
<tr>
<td>5</td>
<td>Designated Approving Authority (DAA)</td>
</tr>
<tr>
<td>5</td>
<td>Technical Support Personnel</td>
</tr>
<tr>
<td>3</td>
<td>Records Management Official</td>
</tr>
<tr>
<td>3</td>
<td>Source Selection Board Member</td>
</tr>
<tr>
<td>2</td>
<td>Freedom of Information Act Official</td>
</tr>
<tr>
<td>2</td>
<td>Privacy Act Official</td>
</tr>
<tr>
<td>2</td>
<td>Telecommunications Specialist</td>
</tr>
</tbody>
</table>

* Includes Information System Security Officer (ISSO), Network Security Officer (NSO), AIS Computer Security Officer (ACSO), Computer Security Officer (CSO), and other similar titles agencies may designate.
Exhibit 4-4

IT Security Body of Knowledge Topics and Concepts


1. LAWS AND REGULATIONS

Federal government-wide and organization-specific laws, regulations, policies, guidelines, standards, and procedures mandating requirements for the management and protection of information technology resources.

- Federal Laws and Regulations
- Federal Standards and Guidelines
- Legal and Liability Issues
- Organization Policy, Guidelines, Standards and Procedures Development
- Organization Program
- Issue-specific
- System-specific

2. IT SECURITY PROGRAM

A program established, implemented, and maintained to assure that adequate IT security is provided for all organizational information collected, processed, transmitted, stored, or disseminated in its general support systems and major applications.

- Organization-wide IT Security Program
- System-level IT Security Program
- Elements of IT Security Program
- Roles, Responsibilities, and Accountability
  - Senior Management
  - Organization-wide IT Security Managers
  - Program and Functional Managers
  - System/Application Owners
  - Information Owner/Custodian
  - IT System Security Managers
  - Contractors
  - Related Security Program Managers
  - Users
### Exhibit 4-4 (Continued)
**IT Security Body of Knowledge Topics and Concepts**

<table>
<thead>
<tr>
<th>3. SYSTEM ENVIRONMENT</th>
</tr>
</thead>
<tbody>
<tr>
<td>The unique technical and operating characteristics of an IT system and its associated environment, including the hardware, software, firmware, communications capability, and physical location.</td>
</tr>
<tr>
<td>IT Architecture</td>
</tr>
<tr>
<td>Hardware Types</td>
</tr>
<tr>
<td>Operating Software</td>
</tr>
<tr>
<td>Application Software</td>
</tr>
<tr>
<td>Communication Requirements</td>
</tr>
<tr>
<td>Facilities Planning</td>
</tr>
<tr>
<td>Processing Workflow</td>
</tr>
<tr>
<td>Utility Software</td>
</tr>
<tr>
<td>Associated Threats</td>
</tr>
<tr>
<td>Associated Vulnerabilities</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>4. SYSTEM INTERCONNECTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>The requirements for communication or interconnection by an IT system with one or more other IT systems or networks, to share processing capability or pass data and information in support of multi-organizational or public programs.</td>
</tr>
<tr>
<td>Communications Types</td>
</tr>
<tr>
<td>Network Architecture</td>
</tr>
<tr>
<td>Electronic Mail</td>
</tr>
<tr>
<td>Electronic Commerce</td>
</tr>
<tr>
<td>Electronic Funds Transfer</td>
</tr>
<tr>
<td>Electronic Data Interchange</td>
</tr>
<tr>
<td>Digital Signatures</td>
</tr>
<tr>
<td>Electronic Signatures</td>
</tr>
<tr>
<td>Access Controls (e.g., firewalls, proxy servers, dedicated circuits)</td>
</tr>
<tr>
<td>Monitoring</td>
</tr>
<tr>
<td>Cryptography</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>5. INFORMATION SHARING</th>
</tr>
</thead>
<tbody>
<tr>
<td>The requirements for information sharing by an IT system with one or more other IT systems or applications, for information sharing to support multiple internal or external organizations, missions, or public programs.</td>
</tr>
<tr>
<td>Communications Types</td>
</tr>
<tr>
<td>Network Architecture</td>
</tr>
<tr>
<td>Electronic Mail</td>
</tr>
<tr>
<td>Electronic Commerce</td>
</tr>
<tr>
<td>Electronic Funds Transfer</td>
</tr>
<tr>
<td>Electronic Data Interchange</td>
</tr>
<tr>
<td>Digital Signatures</td>
</tr>
<tr>
<td>Electronic Signatures</td>
</tr>
<tr>
<td>Access Controls (e.g., Firewalls, Proxy servers, Dedicated circuits)</td>
</tr>
<tr>
<td>Monitoring</td>
</tr>
<tr>
<td>Cryptography</td>
</tr>
<tr>
<td>Data Ownership</td>
</tr>
<tr>
<td>Protection and Labeling of Data Storage Media</td>
</tr>
</tbody>
</table>
### Exhibit 4-4 (Continued)
#### IT Security Body of Knowledge Topics and Concepts

<table>
<thead>
<tr>
<th>6. SENSITIVITY</th>
</tr>
</thead>
<tbody>
<tr>
<td>An IT environment consists of the system, data, and applications which must be examined individually and in total. All IT systems and applications require some level of protection (to ensure confidentiality, integrity, and availability) which is determined by an evaluation of the sensitivity and criticality of the information processed, the relation of the system to the organization missions and the economic value of the system components.</td>
</tr>
<tr>
<td>Confidentiality</td>
</tr>
<tr>
<td>Integrity</td>
</tr>
<tr>
<td>Availability</td>
</tr>
<tr>
<td>Criticality</td>
</tr>
<tr>
<td>Aggregation</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>7. RISK MANAGEMENT</th>
</tr>
</thead>
<tbody>
<tr>
<td>The on-going process of assessing the risk to IT resources and information, as part of a risk-based approach used to determine adequate security for a system, by analyzing the threats and vulnerabilities and selecting appropriate cost-effective controls to achieve and maintain an acceptable level of risk.</td>
</tr>
<tr>
<td>Risk Assessment</td>
</tr>
<tr>
<td>Risk Analysis</td>
</tr>
<tr>
<td>Risk Mitigation</td>
</tr>
<tr>
<td>Uncertainty Analysis</td>
</tr>
<tr>
<td>Threats</td>
</tr>
<tr>
<td>Vulnerabilities</td>
</tr>
<tr>
<td>Risks</td>
</tr>
<tr>
<td>Probability Estimation</td>
</tr>
<tr>
<td>Rate of Occurrence</td>
</tr>
<tr>
<td>Asset Valuation</td>
</tr>
<tr>
<td>Adequate and Appropriate Protection of Assets</td>
</tr>
<tr>
<td>Cost Effectiveness</td>
</tr>
<tr>
<td>Cost-Benefit Analysis</td>
</tr>
<tr>
<td>Application Security Reviews/Audits</td>
</tr>
<tr>
<td>System Security Reviews/Audits</td>
</tr>
<tr>
<td>Verification Reviews</td>
</tr>
<tr>
<td>Internal Control Reviews</td>
</tr>
<tr>
<td>EDP Audits</td>
</tr>
</tbody>
</table>
Exhibit 4-4 (Continued)

IT Security Body of Knowledge Topics and Concepts

8. MANAGEMENT CONTROLS

Management controls are actions taken to manage the development, maintenance, and use of the system, including system-specific policies, procedures, and rules of behavior, individual roles and responsibilities, individual accountability and personnel security decisions.

System/Application Responsibilities
- Program and Functional Managers
- Owners
- Custodians
- Contractors
- Related Security Program Managers
- IT System Security Manager
- Users

System/Application-Specific Policies and Procedures
- Standard Operating Procedures

Personnel Security
- Background Investigations
- Position Sensitivity
- Separation of Duties/Compartmentalization

System Rules of Behavior
- Assignment and Limitation of System Privileges
- Connection to Other Systems and Networks
- Intellectual Property/Copyright Issues
- Remote Access/Work at Home Issues
- Official vs. Unofficial System Use
- Individual Accountability
- Sanctions or Penalties for Violations

9. ACQUISITION/DEVELOPMENT/INSTALLATION/IMPLEMENTATION CONTROLS

The process of assuring that adequate controls are considered, evaluated, selected, designed and built into the system during its early planning and development stages and that an on-going process is established to ensure continued operation at an acceptable level of risk during the installation, implementation and operation stages.

Life Cycle Planning
- Security Activities in Life Cycle Stages
- Security Plan Development and Maintenance
- Security Specifications
- Configuration Management
- Change Control Procedures
- Design Review and Testing
- Authority to Operate
  - Certification/Recertification
  - Accreditation/Re-accreditation
- Acquisition Specifications
- Contracts, Agreements and Other Obligations
- Acceptance Testing
- Prototyping
## Exhibit 4-4  (Continued)

### IT Security Body of Knowledge Topics and Concepts

<table>
<thead>
<tr>
<th>10. OPERATIONAL CONTROLS</th>
</tr>
</thead>
<tbody>
<tr>
<td>The day-to-day procedures and mechanisms used to protect operational systems and applications. Operational controls affect the system and application environment.</td>
</tr>
<tr>
<td>Physical and Environmental Protection</td>
</tr>
<tr>
<td>Physical Security Program</td>
</tr>
<tr>
<td>Environmental Controls</td>
</tr>
<tr>
<td>Natural Threats</td>
</tr>
<tr>
<td>Facility Management</td>
</tr>
<tr>
<td>Fire Prevention and Protection</td>
</tr>
<tr>
<td>Electrical/Power</td>
</tr>
<tr>
<td>Housekeeping</td>
</tr>
<tr>
<td>Physical Access Controls</td>
</tr>
<tr>
<td>Intrusion Detection/Alarms</td>
</tr>
<tr>
<td>Maintenance</td>
</tr>
<tr>
<td>Water/Plumbing</td>
</tr>
<tr>
<td>Mobile and Portable, Systems</td>
</tr>
<tr>
<td>Production, Input/Output Controls</td>
</tr>
<tr>
<td>Document Labeling, Handling, Shipping and Storing</td>
</tr>
<tr>
<td>Media Labeling, Handling, Shipping and Storing</td>
</tr>
<tr>
<td>Disposal of Sensitive Material</td>
</tr>
<tr>
<td>Magnetic Remnance - Cleaning and Clearing</td>
</tr>
<tr>
<td>Contingency Planning</td>
</tr>
<tr>
<td>Backups</td>
</tr>
<tr>
<td>Contingency/Disaster Recovery Plan Development</td>
</tr>
<tr>
<td>Contingency/Disaster Recovery Plan Testing</td>
</tr>
<tr>
<td>Contracting for Contingency Services</td>
</tr>
<tr>
<td>Contracting for Disaster Recovery Services</td>
</tr>
<tr>
<td>Insurance/Government Self-Insurance</td>
</tr>
<tr>
<td>Audit and Variance Detection</td>
</tr>
<tr>
<td>System Logs and Records</td>
</tr>
<tr>
<td>Deviations from Standard Activity</td>
</tr>
<tr>
<td>Hardware and System Software Maintenance Controls</td>
</tr>
<tr>
<td>Application Software Maintenance Controls</td>
</tr>
<tr>
<td>Documentation</td>
</tr>
</tbody>
</table>

| 11. AWARENESS, TRAINING, AND EDUCATION CONTROLS |
| (1) Awareness programs set the stage for training by changing organizational attitudes to realize the importance of security and the adverse consequences of its failure. (2) The purpose of training is to teach people the skills that will enable them to perform their jobs more effectively. (3) Education is targeted for IT security professionals and focuses on developing the ability and vision to perform complex, multi-disciplinary activities. |
### Exhibit 4-4  (Continued)
**IT Security Body of Knowledge Topics and Concepts**

#### 12. TECHNICAL CONTROLS

Technical controls consist of hardware and software controls used to provide automated protection to the IT system or applications. Technical controls operate within the technical system and applications.

- **User Identification and Authentication**
  - Passwords
  - Tokens
  - Biometrics
  - Single Log-in

- **Authorization/Access Controls**
  - Logical Access Controls
  - Role-Based Access
  - System/Application Privileges

- **Integrity/Validation Controls**
  - Compliance with Security Specifications and Requirements
  - Malicious Program/Virus Protection, Detection and Removal
  - Authentication Messages
  - Reconciliation Routines

- **Audit Trail Mechanisms**
  - Transaction Monitoring
  - Reconstruction of Transactions

- **Confidentiality Controls**
  - Cryptography

- **Incident Response**
  - Fraud, Waste or Abuse
  - Hackers and Unauthorized User Activities
  - Incident Reporting
  - Incident Investigation
  - Prosecution

- **Public Access Controls**
  - Access Controls
  - Need-to-know
  - Privileges

- **Control Objectives**
  - Protection Requirements
SECTION 4.2

IT SECURITY TRAINING MATRIX CELLS

(See Appendix B for a full-page illustration of the IT Security Training Matrix)
SECTION 4.2.1

TRAINING AREA:
LAWS AND REGULATIONS
# INFORMATION TECHNOLOGY SECURITY TRAINING MATRIX — **Cell 1A**

<table>
<thead>
<tr>
<th>Training Area: <strong>Laws &amp; Regulations</strong></th>
<th>Functional Specialty: <strong>Manage</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Definition</strong> — Federal government-wide and organization-specific published documents (laws, regulations, policies, guidelines, standards, and codes of conduct) governing mandated requirements and standards for the management and protection of information technology resources.</td>
<td></td>
</tr>
</tbody>
</table>

**Behavioral Outcome** — Managers are able to understand applicable governing documents and their interrelationships and interpret and apply them to the manager’s area of responsibility.

**Knowledge Levels** —

1. **Beginning** — Research, Know, Identify
2. **Intermediate** — Analyze, Understand, Apply
3. **Advanced** — Interpret, Approve, Decide, Issue

**Sample Learning Objectives** —

At the conclusion of this module, individuals will be able to:

1. **Beginning** — Know where to find Federal government-wide and organization-specific published documents, such as laws, regulations, policies, guidelines, and standards (e.g., the Computer Security Act of 1987) and how to apply them.

2. **Intermediate** — Develop policies that reflect the legislative intent of applicable laws and regulations (e.g., policies addressing software copyright law infringement).

3. **Advanced** — Analyze, approve, and issue policies (e.g., authorizes policies as part of an IRM manual).

**Sample Job Functions** —

- Chief Information Officer (CIO)
- Information Resources Management (IRM) Official, Senior
- Information Resources Manager
- IT Security Officer/Manager
<table>
<thead>
<tr>
<th>Training Area: Laws &amp; Regulations</th>
<th>Functional Specialty: Manage</th>
</tr>
</thead>
</table>

**IT SECURITY BODY OF KNOWLEDGE TOPICS AND CONCEPTS**

- 1 — LAWS AND REGULATIONS
- 2 — IT SECURITY PROGRAM
- 7 — RISK MANAGEMENT

*For the content of the numbered topics and concepts above, refer to Exhibit 4-4.*
| Training Area: **Laws & Regulations**  
| Functional Specialty: **Acquire** |
| **Definition** — Federal government-wide and organization-specific published documents (laws, regulations, policies, guidelines, standards, and codes of conduct) governing mandated requirements and standards for the management and protection of information technology resources. |
| **Behavioral Outcome** — Individuals involved in the acquisition of information technology resources have a sufficient understanding of IT security requirements and issues to protect the government’s interest in such acquisitions. |
| **Knowledge Levels** —  
| 1. Beginning — Identify, Know, Research  
| 2. Intermediate — Analyze, Interpret, Develop, Decide  
| 3. Advanced — Evaluate, Approve, Issue |
| **Sample Learning Objectives** —  
| At the conclusion of this module, individuals will be able to:  
| 1. Beginning — Identify security requirements to be included in statements of work and other appropriate procurement documents (e.g., procurement requests, purchase orders, task orders, and proposal evaluation summaries) as required by the Federal regulations.  
| 2. Intermediate — Develop security requirements specific to an information technology acquisition for inclusion in procurement documents (e.g., ensures that required controls are adequate and appropriate) as required by the Federal regulations.  
| 3. Advanced — Evaluate proposals to determine if proposed security solutions effectively address agency requirements as detailed in solicitation documents and are in compliance with Federal regulations. |
| **Sample Job Functions** —  
| • Contracting Officer  
| • Contracting Officer’s Technical Representative (COTR)  
| • Information Resources Management (IRM) Official, Senior  
| • IT Security Officer/Manager  
| • Source Selection Board Member |
### INFORMATION TECHNOLOGY SECURITY TRAINING MATRIX — Cell 1B

**Training Area:** Laws & Regulations  
**Functional Specialty:** Acquire

#### IT SECURITY BODY OF KNOWLEDGE TOPICS AND CONCEPTS

- 1 — LAWS AND REGULATIONS
- 3 — SYSTEM ENVIRONMENT
- 5 — INFORMATION SHARING
- 6 — SENSITIVITY
- 7 — RISK MANAGEMENT
- 8 — MANAGEMENT CONTROLS
- 9 — ACQUISITION/DEVELOPMENT/INSTALLATION/IMPLEMENTATION CONTROLS

*For the content of the numbered topics and concepts above, refer to Exhibit 4-4.*
| Training Area: **Laws & Regulations**  
Functional Specialty: **Design & Develop** |
<table>
<thead>
<tr>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Definition</strong> — Federal government-wide and organization-specific published documents (laws, regulations, policies, guidelines, standards, and codes of conduct) governing mandated requirements and standards for the management and protection of information technology resources.</td>
</tr>
<tr>
<td><strong>Behavioral Outcome</strong> — Individuals responsible for the design and development of automated information systems are able to translate IT laws and regulations into technical specifications which provide adequate and appropriate levels of protection.</td>
</tr>
</tbody>
</table>
| **Knowledge Levels** —  
1. Beginning — Identify, Know, Apply  
2. Intermediate — Research, Interpret, Develop  
3. Advanced — Evaluate, Approve, Select |
| **Sample Learning Objectives** —  
At the conclusion of this module, individuals will be able to:  
1. Beginning — Identify laws and regulations relevant to the specific system being designed (e.g., a financial management system would be subject to the requirements of the Accounting and Auditing Act, whereas a personnel system would be subject to the requirements of the Privacy Act).  
2. Intermediate — Interpret applicable laws and regulations to develop security functional requirements (e.g., requiring encryption for Privacy Act data stored on a shared file server).  
3. Advanced — Evaluate conflicting functional requirements (e.g., the level of audit trail that can be incorporated without adversely affecting system performance) and select for implementation those requirements that will provide the highest level of security at the minimum cost consistent with applicable laws and regulations. |
| **Sample Job Functions** —  
- Auditor, Internal  
- Information Resources Manager  
- IT Security Officer/Manager  
- Program Manager  
- Programmer/Systems Analyst  
- System Designer/Developer |
INFORMATION TECHNOLOGY SECURITY TRAINING MATRIX — Cell 1C

Training Area: Laws & Regulations
Functional Specialty: Design & Develop

IT SECURITY BODY OF KNOWLEDGE TOPICS AND CONCEPTS

- 1 — LAWS AND REGULATIONS
- 2 — IT SECURITY PROGRAM
- 3 — SYSTEM ENVIRONMENT
- 4 — SYSTEM INTERCONNECTION
- 5 — INFORMATION SHARING
- 6 — SENSITIVITY
- 9 — ACQUISITION/DEVELOPMENT/INSTALLATION/IMPLEMENTATION CONTROLS

For the content of the numbered topics and concepts above, refer to Exhibit 4-4.
### Information Technology Security Training Matrix — Cell 1D

| Training Area: **Laws & Regulations** |
| Functional Specialty: **Implement & Operate** |

**Definition** — Federal government-wide and organization-specific published documents (laws, regulations, policies, guidelines, standards, and codes of conduct) governing mandated requirements and standards for the management and protection of information technology resources.

**Behavioral Outcome** — Individuals responsible for the technical implementation and daily operations of an automated information system are able to understand IT security laws and regulations in sufficient detail to ensure that appropriate safeguards are in place and enforced.

**Knowledge Levels** —

1. Beginning — Know, Identify, Apply
2. Intermediate — Investigate, Interpret, Decide, Analyze
3. Advanced — Evaluate, Decide, Approve

**Sample Learning Objectives** —

At the conclusion of this module, individuals will be able to:

1. Beginning — Recognize a potential security violation and take appropriate action to report the incident as required by Federal regulation and mitigate any adverse impact (e.g., block access to a communications port which has been subject to multiple invalid log-on attempts during non-duty hours).

2. Intermediate — Investigate a potential security violation to determine if the organization’s policy has been breached and assess the impact of the breach (e.g., review audit trails to determine if inappropriate access has occurred).

3. Advanced — Determine whether a security breach is indicative of a violation of law that requires specific legal action (e.g., unauthorized access and alteration of data) and forward evidence to the Federal Bureau of Investigation for investigation.

**Sample Job Functions** —

- IT Security Officer/Manager
- Programmer/Systems Analyst
- System Administrator
- Systems Operations Personnel
- Technical Support Personnel
- Network Administrator
<table>
<thead>
<tr>
<th>Training Area: Laws &amp; Regulations</th>
<th>Functional Specialty: Implement &amp; Operate</th>
</tr>
</thead>
</table>

**IT SECURITY BODY OF KNOWLEDGE TOPICS AND CONCEPTS**

- 1 — LAWS AND REGULATIONS
- 7 — RISK MANAGEMENT
- 8 — MANAGEMENT CONTROLS
- 10 — OPERATIONAL CONTROLS
- 12 — TECHNICAL CONTROLS

*For the content of the numbered topics and concepts above, refer to Exhibit 4-4.*
### INFORMATION TECHNOLOGY SECURITY TRAINING MATRIX — **Cell 1E**

<table>
<thead>
<tr>
<th>Training Area: <strong>Laws &amp; Regulations</strong></th>
<th>Functional Specialty: <strong>Review &amp; Evaluate</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Definition</strong> — Federal government-wide and organization-specific published documents (laws, regulations, policies, guidelines, standards, and codes of conduct) governing mandated requirements and standards for the management and protection of information technology resources.</td>
<td></td>
</tr>
<tr>
<td><strong>Behavioral Outcome</strong> — Individuals responsible for the review/evaluation of an automated information system are able to use IT security laws and regulations in developing a comparative baseline and determining the level of system compliance.</td>
<td></td>
</tr>
<tr>
<td><strong>Knowledge Levels</strong> —</td>
<td></td>
</tr>
<tr>
<td>1. Beginning — Identify, Know, Apply</td>
<td></td>
</tr>
<tr>
<td>2. Intermediate — Develop, Interpret, Understand</td>
<td></td>
</tr>
<tr>
<td>3. Advanced — Evaluate, Decide, Approve</td>
<td></td>
</tr>
<tr>
<td><strong>Sample Learning Objectives</strong> —</td>
<td></td>
</tr>
<tr>
<td>At the conclusion of this module, individuals will be able to:</td>
<td></td>
</tr>
<tr>
<td>1. Beginning — Identify laws and regulations applicable to a specific information system or application (e.g., a payroll application is subject to OMB Circulars A-123, A-127, and A-130, while a project management system may only be subject to OMB Circular A-130).</td>
<td></td>
</tr>
<tr>
<td>2. Intermediate — Use laws, regulations, and agency guidance to develop a comparative IT security requirements baseline appropriate to evaluate the existing security environment.</td>
<td></td>
</tr>
<tr>
<td>3. Advanced — Evaluate in-place controls and countermeasures against the comparative baseline to determine if the controls provide a security environment equal to or better than the baseline environment.</td>
<td></td>
</tr>
<tr>
<td><strong>Sample Job Functions</strong> —</td>
<td></td>
</tr>
<tr>
<td>• Auditor, External</td>
<td></td>
</tr>
<tr>
<td>• Auditor, Internal</td>
<td></td>
</tr>
<tr>
<td>• Certification Reviewer</td>
<td></td>
</tr>
<tr>
<td>• Information Resources Manager</td>
<td></td>
</tr>
<tr>
<td>• IT Security Officer/Manager</td>
<td></td>
</tr>
<tr>
<td>Training Area: <strong>Laws &amp; Regulations</strong></td>
<td></td>
</tr>
<tr>
<td>--------------------------------------</td>
<td></td>
</tr>
<tr>
<td>Functional Specialty: <strong>Review &amp; Evaluate</strong></td>
<td></td>
</tr>
</tbody>
</table>

**IT SECURITY BODY OF KNOWLEDGE TOPICS AND CONCEPTS**

- 1 — LAWS AND REGULATIONS
- 3 — SYSTEM ENVIRONMENT
- 4 — SYSTEM INTERCONNECTION
- 5 — INFORMATION SHARING
- 6 — SENSITIVITY
- 7 — RISK MANAGEMENT
- 8 — MANAGEMENT CONTROLS
- 9 — ACQUISITION/DEVELOPMENT/INSTALLATION/IMPLEMENTATION CONTROLS
- 10 — OPERATIONAL CONTROLS
- 11 — AWARENESS, TRAINING, AND EDUCATION CONTROLS
- 12 — TECHNICAL CONTROLS

*For the content of the numbered topics and concepts above, refer to Exhibit 4-4.*
### INFORMATION TECHNOLOGY SECURITY TRAINING MATRIX — **Cell 1F**

<table>
<thead>
<tr>
<th>Training Area: <strong>Laws &amp; Regulations</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Functional Specialty:</strong> <strong>Use</strong></td>
</tr>
</tbody>
</table>

**Definition** — Federal government-wide and organization-specific published documents (laws, regulations, policies, guidelines, standards, and codes of conduct) governing mandated requirements and standards for the management and protection of information technology resources.

**Behavioral Outcome** — Users understand individual accountability and applicable governing documents (e.g., Computer Security Act, Computer Fraud and Abuse Act, Copyright Act, Privacy Act).

**Knowledge Levels** —
1. Beginning — Know, Apply
2. Intermediate/Advanced — Review, Assess, Decide

**Sample Learning Objectives** —

At the conclusion of this module, individuals will be able to:

1. Beginning — Understand that violating applicable laws and regulations (e.g., making unauthorized copies of copyrighted software) can result in assessment of monetary penalties against individuals and the organization.

2. Intermediate/Advanced — Review personal practices to ensure compliance with applicable laws and regulations (e.g., review installed software on the computer for which he or she is responsible to ensure that each software product has an appropriate license).

**Sample Job Functions** —

- Information Resources Manager
- IT Security Officer/Manager
- System Owner
- User
### INFORMATION TECHNOLOGY SECURITY TRAINING MATRIX — Cell 1F

<table>
<thead>
<tr>
<th>Training Area: Laws &amp; Regulations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Functional Specialty: Use</td>
</tr>
</tbody>
</table>

#### IT SECURITY BODY OF KNOWLEDGE TOPICS AND CONCEPTS

- **1** — LAWS AND REGULATIONS
- **8** — MANAGEMENT CONTROLS

*For the content of the numbered topics and concepts above, refer to *Exhibit 4-4.*"
SECTION 4.2.2

TRAINING AREA: SECURITY PROGRAM
## INFORMATION TECHNOLOGY SECURITY TRAINING MATRIX — Cell 2.1A

<table>
<thead>
<tr>
<th>Training Area: Security Program — Planning</th>
<th>Functional Specialty: Manage</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Definition</strong> — The design and establishment of organizational structures and processes for IT security program goal-setting, prioritizing, and related decision-making activities; these encompass such elements as organization-specific scope and content, including: policy, guidelines, needs identification, roles, responsibilities, and resource allocation.</td>
<td></td>
</tr>
<tr>
<td><strong>Behavioral Outcome</strong> — Individuals involved in the management of IT security programs are able to understand principles and processes of program planning and can organize resources to develop a security program that meets organizational needs.</td>
<td></td>
</tr>
<tr>
<td><strong>Knowledge Levels</strong> —</td>
<td></td>
</tr>
<tr>
<td>1. Beginning — Participate, Know, Apply</td>
<td></td>
</tr>
<tr>
<td>2. Intermediate — Interpret, Develop, Decide</td>
<td></td>
</tr>
<tr>
<td>3. Advanced — Evaluate, Approve, Direct</td>
<td></td>
</tr>
<tr>
<td><strong>Sample Learning Objectives</strong> —</td>
<td></td>
</tr>
<tr>
<td>At the conclusion of this module, individuals will be able to:</td>
<td></td>
</tr>
<tr>
<td>1. Beginning — Participate in the development or modification of the organization’s IT security program plans and requirements.</td>
<td></td>
</tr>
<tr>
<td>2. Intermediate — Develop and/or modify IT security program policy, guidelines, and procedures and recommend associated resource allocations.</td>
<td></td>
</tr>
<tr>
<td>3. Advanced — Identify IT security program implications of new technologies or technology upgrades. Review and approve various IT security plans for appropriateness and effectiveness. Set priorities for allocation of resources.</td>
<td></td>
</tr>
<tr>
<td><strong>Sample Job Functions</strong> —</td>
<td></td>
</tr>
<tr>
<td>• Information Resources Manager</td>
<td></td>
</tr>
<tr>
<td>• IT Security Officer/Manager</td>
<td></td>
</tr>
<tr>
<td>• Program Manager</td>
<td></td>
</tr>
<tr>
<td>• System Owner</td>
<td></td>
</tr>
<tr>
<td>Training Area: <strong>Security Program — Planning</strong></td>
<td>Functional Specialty: <strong>Manage</strong></td>
</tr>
<tr>
<td>-----------------------------------------------</td>
<td>---------------------------------</td>
</tr>
</tbody>
</table>

**IT SECURITY BODY OF KNOWLEDGE TOPICS AND CONCEPTS**

- 1 — LAWS AND REGULATIONS
- 2 — IT SECURITY PROGRAM
- 3 — SYSTEM ENVIRONMENT
- 4 — SYSTEM INTERCONNECTION
- 5 — INFORMATION SHARING
- 6 — SENSITIVITY
- 7 — RISK MANAGEMENT
- 8 — MANAGEMENT CONTROLS
- 9 — ACQUISITION/DEVELOPMENT/INSTALLATION/IMPLEMENTATION CONTROLS
- 10 — OPERATIONAL CONTROLS
- 11 — AWARENESS, TRAINING, AND EDUCATION CONTROLS
- 12 — TECHNICAL CONTROLS

*For the content of the numbered topics and concepts above, refer to Exhibit 4-4.*
## INFORMATION TECHNOLOGY SECURITY TRAINING MATRIX — Cell 2.1B

<table>
<thead>
<tr>
<th>Training Area: Security Program — Planning</th>
<th>Functional Specialty: Acquire</th>
</tr>
</thead>
</table>

### Definition —
The design and establishment of organizational structures and processes for IT security program goal-setting, prioritizing, and related decision-making activities; these encompass such elements as organization-specific scope and content, including: policy, guidelines, needs identification, roles, responsibilities, and resource allocation.

### Behavioral Outcome —
Individuals involved in planning the IT security program can identify the resources required for successful implementation. Individuals recognize the need to include IT security requirements in IT acquisitions and to incorporate appropriate acquisition policy and oversight in the IT security program.

### Knowledge Levels —
1. Beginning/Intermediate — Develop, Interpret, Decide, Apply
2. Advanced — Evaluate, Interpret, Approve, Issue

### Sample Learning Objectives —
At the conclusion of this module, individuals will be able to:

1. Beginning/Intermediate — Develop security requirements for hardware, software, and services acquisitions specific to the IT security program (e.g., purchase of virus-scanning software or security reviews) and for inclusion in general IT acquisition guidance.

2. Advanced — Interpret and/or approve security requirements relative to the capabilities of new information technologies, revise IT acquisition guidance as appropriate, and issue changes.

### Sample Job Functions —
- Contracting Officer’s Technical Representative (COTR)
- Information Resources Manager
- IT Security Officer/Manager
- Source Selection Board Member
- Telecommunications Specialist
<table>
<thead>
<tr>
<th>Cell 2.1B</th>
</tr>
</thead>
<tbody>
<tr>
<td>INTEGRATION TECHNOLOGY SECURITY TRAINING MATRIX</td>
</tr>
<tr>
<td>Training Area: Security Program — Planning</td>
</tr>
<tr>
<td>Functional Specialty: Acquire</td>
</tr>
</tbody>
</table>

**IT SECURITY BODY OF KNOWLEDGE TOPICS AND CONCEPTS**

- 2 — IT SECURITY PROGRAM
- 3 — SYSTEM ENVIRONMENT
- 4 — SYSTEM INTERCONNECTION
- 5 — INFORMATION SHARING
- 9 — ACQUISITION/DEVELOPMENT/INSTALLATION/IMPLEMENTATION CONTROLS
- 10 — OPERATIONAL CONTROLS
- 12 — TECHNICAL CONTROLS

*For the content of the numbered topics and concepts above, refer to Exhibit 4-4.*
<table>
<thead>
<tr>
<th>INFORMATION TECHNOLOGY SECURITY TRAINING MATRIX — <strong>Cell 2.1C</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Training Area:</strong> Security Program — Planning</td>
</tr>
<tr>
<td><strong>Functional Specialty:</strong> Design &amp; Develop</td>
</tr>
<tr>
<td><strong>Definition</strong> — The design and establishment of organizational structures and processes for IT security program goal-setting, prioritizing, and related decision-making activities; these encompass such elements as organization-specific scope and content, including: policy, guidelines, needs identification, roles, responsibilities, and resource allocation.</td>
</tr>
<tr>
<td><strong>Behavioral Outcome</strong> — Individuals responsible for the design and development of an IT security program are able to create a security program plan specific to a business process or organizational entity.</td>
</tr>
<tr>
<td><strong>Knowledge Levels</strong> —</td>
</tr>
<tr>
<td>1. Beginning — Locate, Understand, Apply</td>
</tr>
<tr>
<td>2. Intermediate/Advanced — Design, Develop, Decide</td>
</tr>
<tr>
<td><strong>Sample Learning Objectives</strong> —</td>
</tr>
<tr>
<td>At the conclusion of this module, individuals will be able to:</td>
</tr>
<tr>
<td>1. Beginning — Understand the various components of an effective IT security program and relate them to the organization’s business process requirements.</td>
</tr>
<tr>
<td>2. Intermediate/Advanced — Design, develop, or modify IT security program requirements.</td>
</tr>
<tr>
<td><strong>Sample Job Functions</strong> —</td>
</tr>
<tr>
<td>• Chief Information Officer (CIO)</td>
</tr>
<tr>
<td>• Information Resources Manager</td>
</tr>
<tr>
<td>• IT Security Officer/Manager</td>
</tr>
</tbody>
</table>
INFORMATION TECHNOLOGY SECURITY TRAINING MATRIX — Cell 2.1C

Training Area: Security Program — Planning
Functional Specialty: Design & Develop

IT SECURITY BODY OF KNOWLEDGE TOPICS AND CONCEPTS

- 2 — IT SECURITY PROGRAM
- 3 — SYSTEM ENVIRONMENT
- 4 — SYSTEM INTERCONNECTION
- 5 — INFORMATION SHARING
- 6 — SENSITIVITY
- 7 — RISK MANAGEMENT
- 8 — MANAGEMENT CONTROLS
- 9 — ACQUISITION/DEVELOPMENT/INSTALLATION/IMPLEMENTATION CONTROLS
- 10 — OPERATIONAL CONTROLS
- 11 — AWARENESS, TRAINING, AND EDUCATION CONTROLS
- 12 — TECHNICAL CONTROLS

For the content of the numbered topics and concepts above, refer to Exhibit 4-4.
<table>
<thead>
<tr>
<th>INFORMATION TECHNOLOGY SECURITY TRAINING MATRIX — <strong>Cell 2.1D</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Training Area:</strong> <strong>Security Program — Planning</strong></td>
</tr>
<tr>
<td><strong>Functional Specialty:</strong> <strong>Implement &amp; Operate</strong></td>
</tr>
<tr>
<td><strong>Definition</strong> — The design and establishment of organizational structures and processes for IT security program goal-setting, prioritizing, and related decision-making activities; these encompass such elements as organization-specific scope and content, including: policy, guidelines, needs identification, roles, responsibilities, and resource allocation.</td>
</tr>
<tr>
<td><strong>Behavioral Outcome</strong> — Individuals responsible for implementing and operating an IT security program are able to develop plans for security controls, countermeasures, and processes as required to execute the existing program.</td>
</tr>
<tr>
<td><strong>Knowledge Levels</strong> —</td>
</tr>
<tr>
<td>1. Beginning — Understand, Participate, Develop, Apply</td>
</tr>
<tr>
<td>2. Intermediate/Advanced — Approve, Allocate, Interpret, Direct</td>
</tr>
<tr>
<td><strong>Sample Learning Objectives</strong> —</td>
</tr>
<tr>
<td>At the conclusion of this module, individuals will be able to:</td>
</tr>
<tr>
<td>1. Beginning — Participate in the development of plans for implementing IT security program elements (e.g., develop procedures for screening new employees).</td>
</tr>
<tr>
<td>2. Intermediate/Advanced — Develop implementation strategies and resource estimates required to achieve IT security goals. Allocate resources among competing tasks to achieve the maximum level of security at optimum cost.</td>
</tr>
<tr>
<td><strong>Sample Job Functions</strong> —</td>
</tr>
<tr>
<td>• Auditor, Internal</td>
</tr>
<tr>
<td>• Chief Information Officer (CIO)</td>
</tr>
<tr>
<td>• Information Resources Manager</td>
</tr>
<tr>
<td>• IT Security Officer/Manager</td>
</tr>
</tbody>
</table>
### INFORMATION TECHNOLOGY SECURITY TRAINING MATRIX — Cell 2.1D

**Training Area:** Security Program — Planning  
**Functional Specialty:** Implement & Operate

#### IT SECURITY BODY OF KNOWLEDGE TOPICS AND CONCEPTS

- **2** — IT SECURITY PROGRAM  
- **7** — RISK MANAGEMENT  
- **8** — MANAGEMENT CONTROLS  
- **9** — ACQUISITION/DEVELOPMENT/INSTALLATION/IMPLEMENTATION CONTROLS  
- **10** — OPERATIONAL CONTROLS  
- **11** — AWARENESS, TRAINING, AND EDUCATION CONTROLS  
- **12** — TECHNICAL CONTROLS

*For the content of the numbered topics and concepts above, refer to Exhibit 4-4.*
INFORMATION TECHNOLOGY SECURITY TRAINING MATRIX — Cell 2.1E

<table>
<thead>
<tr>
<th>Training Area: <strong>Security Program — Planning</strong></th>
<th>Functional Specialty: <strong>Review &amp; Evaluate</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Definition</strong> — The design and establishment of organizational structures and processes for IT security program goal-setting, prioritizing, and related decision-making activities; these encompass such elements as organization-specific scope and content, including: policy, guidelines, needs identification, roles, responsibilities, and resource allocation.</td>
<td></td>
</tr>
<tr>
<td><strong>Behavioral Outcome</strong> — Individuals responsible for the review/evaluation of an IT security program are able to review the program to determine its continuing capability to cost-effectively address identified requirements.</td>
<td></td>
</tr>
<tr>
<td><strong>Knowledge Levels</strong></td>
<td></td>
</tr>
<tr>
<td>1. Beginning/Intermediate — Review, Know, Interpret</td>
<td></td>
</tr>
<tr>
<td>2. Advanced — Evaluate, Approve, Recommend</td>
<td></td>
</tr>
</tbody>
</table>

**Sample Learning Objectives** —

At the conclusion of this module, individuals will be able to:

1. Beginning/Intermediate — Review the plans for implementing IT security program elements to ensure that they effectively address program objectives.

2. Advanced — Provide recommendations for correcting identified deficiencies. Evaluate action plans for correcting identified deficiencies and provide recommendations for strengthening the IT security program plans.

**Sample Job Functions** —

- Auditor, External
- Auditor, Internal
- CIO
- Information Resources Management (IRM) Official, Senior
- IT Security Officer/Manager
<table>
<thead>
<tr>
<th>Training Area: Security Program — Planning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Functional Specialty: Review &amp; Evaluate</td>
</tr>
</tbody>
</table>

**IT SECURITY BODY OF KNOWLEDGE TOPICS AND CONCEPTS**

- 1 — LAWS AND REGULATIONS
- 2 — IT SECURITY PROGRAM
- 3 — SYSTEM ENVIRONMENT
- 4 — SYSTEM INTERCONNECTION
- 5 — INFORMATION SHARING
- 6 — SENSITIVITY
- 7 — RISK MANAGEMENT
- 8 — MANAGEMENT CONTROLS
- 9 — ACQUISITION/DEVELOPMENT/INSTALLATION/IMPLEMENTATION CONTROLS
- 10 — OPERATIONAL CONTROLS
- 11 — AWARENESS, TRAINING, AND EDUCATION CONTROLS
- 12 — TECHNICAL CONTROLS

*For the content of the numbered topics and concepts above, refer to Exhibit 4-4.*
### INFORMATION TECHNOLOGY SECURITY TRAINING MATRIX — Cell 2.2A

<table>
<thead>
<tr>
<th>Training Area: Security Program — Management</th>
<th>Functional Specialty: Manage</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Definition</strong> — The implementation and use of organizational structures and processes for IT security program goal-setting, prioritizing, and related decision-making activities; these encompass such elements as organization-specific policies, guidelines, requirements, roles, responsibilities, and resource allocation.</td>
<td></td>
</tr>
<tr>
<td><strong>Behavioral Outcome</strong> — Individuals involved in IT security program management understand and are able to implement a security program that meets their organization’s needs.</td>
<td></td>
</tr>
<tr>
<td><strong>Knowledge Levels</strong> —</td>
<td></td>
</tr>
<tr>
<td>1. Beginning — Recognize, Know, Apply</td>
<td></td>
</tr>
<tr>
<td>2. Intermediate — Evaluate, Know, Review</td>
<td></td>
</tr>
<tr>
<td>3. Advanced — Determine, Interpret, Direct</td>
<td></td>
</tr>
<tr>
<td><strong>Sample Learning Objectives</strong> —</td>
<td></td>
</tr>
<tr>
<td>At the conclusion of this module, individuals will be able to:</td>
<td></td>
</tr>
<tr>
<td>1. Beginning — Monitor organizational activities to ensure compliance with the existing IT security program (e.g., ensure that all IT systems have been identified and security plans prepared).</td>
<td></td>
</tr>
<tr>
<td>2. Intermediate — Review organizational IT security plans to ensure that they appropriately address the security requirements of each system.</td>
<td></td>
</tr>
<tr>
<td>3. Advanced — Interpret patterns of non-compliance to determine their impact on levels of risk and/or overall effectiveness of the IT security program and, on that basis, modify or augment the program as appropriate.</td>
<td></td>
</tr>
<tr>
<td><strong>Sample Job Functions</strong> —</td>
<td></td>
</tr>
<tr>
<td>• Chief Information Officer (CIO)</td>
<td></td>
</tr>
<tr>
<td>• Information Resources Manager</td>
<td></td>
</tr>
<tr>
<td>• IT Security Officer/Manager</td>
<td></td>
</tr>
<tr>
<td>• Program Manager</td>
<td></td>
</tr>
<tr>
<td>Cell 2.2A</td>
<td>INFORMATION TECHNOLOGY SECURITY TRAINING MATRIX — Cell 2.2A</td>
</tr>
<tr>
<td>-----------</td>
<td>----------------------------------------------------------</td>
</tr>
<tr>
<td>Training Area: <strong>Security Program — Management</strong></td>
<td></td>
</tr>
<tr>
<td>Functional Specialty: <strong>Manage</strong></td>
<td></td>
</tr>
<tr>
<td><strong>IT SECURITY BODY OF KNOWLEDGE TOPICS AND CONCEPTS</strong></td>
<td></td>
</tr>
<tr>
<td>• 1 — LAWS AND REGULATIONS</td>
<td></td>
</tr>
<tr>
<td>• 2 — IT SECURITY PROGRAM</td>
<td></td>
</tr>
<tr>
<td>• 3 — SYSTEM ENVIRONMENT</td>
<td></td>
</tr>
<tr>
<td>• 4 — SYSTEM INTERCONNECTION</td>
<td></td>
</tr>
<tr>
<td>• 5 — INFORMATION SHARING</td>
<td></td>
</tr>
<tr>
<td>• 6 — SENSITIVITY</td>
<td></td>
</tr>
<tr>
<td>• 7 — RISK MANAGEMENT</td>
<td></td>
</tr>
<tr>
<td>• 8 — MANAGEMENT CONTROLS</td>
<td></td>
</tr>
<tr>
<td>• 9 — ACQUISITION/DEVELOPMENT/INSTALLATION/</td>
<td></td>
</tr>
<tr>
<td>IMPLEMENTATION CONTROLS</td>
<td></td>
</tr>
<tr>
<td>• 10 — OPERATIONAL CONTROLS</td>
<td></td>
</tr>
<tr>
<td>• 11 — AWARENESS, TRAINING, AND EDUCATION CONTROLS</td>
<td></td>
</tr>
<tr>
<td>• 12 — TECHNICAL CONTROLS</td>
<td></td>
</tr>
</tbody>
</table>

*For the content of the numbered topics and concepts above, refer to Exhibit 4-4.*
### INFORMATION TECHNOLOGY SECURITY TRAINING MATRIX — **Cell 2.2B**

<table>
<thead>
<tr>
<th>Training Area: <strong>Security Program — Management</strong></th>
<th>Functional Specialty: <strong>Acquire</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Definition</strong> — The implementation and use of organizational structures and processes for IT security program goal-setting, prioritizing, and related decision-making activities; these encompass such elements as organization-specific policies, guidelines, requirements, roles, responsibilities, and resource allocation.</td>
<td></td>
</tr>
<tr>
<td><strong>Behavioral Outcome</strong> — Individuals involved in managing the IT security program have a sufficient understanding of IT security and the acquisition process to incorporate IT security program requirements into acquisition work steps.</td>
<td></td>
</tr>
<tr>
<td><strong>Knowledge Levels</strong> —</td>
<td></td>
</tr>
<tr>
<td>1. Beginning — Identify, Know, Apply</td>
<td></td>
</tr>
<tr>
<td>2. Intermediate — Define, Develop, Write</td>
<td></td>
</tr>
<tr>
<td>3. Advanced — Evaluate, Determine, Approve</td>
<td></td>
</tr>
<tr>
<td><strong>Sample Learning Objectives</strong> —</td>
<td></td>
</tr>
<tr>
<td>At the conclusion of this module, individuals will be able to:</td>
<td></td>
</tr>
<tr>
<td>1. Beginning — Identify areas within the acquisition process where IT security work steps are required.</td>
<td></td>
</tr>
<tr>
<td>2. Intermediate — Develop security work steps for inclusion in the acquisition process, e.g., requiring an IT Security Officer review of statements of work.</td>
<td></td>
</tr>
<tr>
<td>3. Advanced — Evaluate procurement activities to ensure that IT security work steps are being effectively performed.</td>
<td></td>
</tr>
<tr>
<td><strong>Sample Job Functions</strong> —</td>
<td></td>
</tr>
<tr>
<td>• Contracting Officer</td>
<td></td>
</tr>
<tr>
<td>• Contracting Officer’s Technical Representative (COTR)</td>
<td></td>
</tr>
<tr>
<td>• Information Resources Manager</td>
<td></td>
</tr>
<tr>
<td>• IT Security Officer/Manager</td>
<td></td>
</tr>
<tr>
<td>• Source Selection Board Member</td>
<td></td>
</tr>
</tbody>
</table>
# INFORMATION TECHNOLOGY SECURITY TRAINING MATRIX — **Cell 2.2B**

**Training Area:** Security Program — Management  
**Functional Specialty:** Acquire

## IT SECURITY BODY OF KNOWLEDGE TOPICS AND CONCEPTS

- **1** — LAWS AND REGULATIONS  
- **2** — IT SECURITY PROGRAM  
- **3** — SYSTEM ENVIRONMENT  
- **9** — ACQUISITION/DEVELOPMENT/INSTALLATION/IMPLEMENTATION CONTROLS

For the content of the numbered topics and concepts above, refer to *Exhibit 4-4.*
INFORMATION TECHNOLOGY SECURITY TRAINING MATRIX — **Cell 2.2C**

**Training Area:** Security Program — Management  
**Functional Specialty:** Design & Develop

**Definition** — The implementation and use of organizational structures and processes for IT security program goal-setting, prioritizing, and related decision-making activities; these encompass such elements as organization-specific policies, guidelines, requirements, roles, responsibilities, and resource allocation.

**Behavioral Outcome** — Individuals responsible for the design and development of an IT security program have sufficient understanding of the appropriate program elements and requirements to be able to translate them into detailed policies and procedures which provide adequate and appropriate protection for the organization’s IT resources in relation to acceptable levels of risk.

**Knowledge Levels** —

1. Beginning — Know, Research, Understand  
2. Intermediate — Interpret, Decide, Establish, Apply  
3. Advanced — Analyze, Interpret, Approve, Direct

**Sample Learning Objectives** —

At the conclusion of this module, individuals will be able to:

1. Beginning — Understand categories of risk and participate in the design and development of operational IT security program procedures.

2. Intermediate — Establish acceptable levels of risk and translate the IT security program elements into operational procedures for providing adequate and appropriate protection of the organization’s IT resources.

3. Advanced — Design, develop, and direct the activities necessary to marshal the organizational structures, processes, and people for an effective IT security program implementation.

**Sample Job Functions** —

- Chief Information Officer (CIO)  
- Information Resources Management (IRM) Official, Senior  
- IT Security Officer/Manager
### INFORMATION TECHNOLOGY SECURITY TRAINING MATRIX — Cell 2.2C

**Training Area:** Security Program — Management  
**Functional Specialty:** Design & Develop

**IT SECURITY BODY OF KNOWLEDGE TOPICS AND CONCEPTS**

- 2  —  IT SECURITY PROGRAM  
- 7  —  RISK MANAGEMENT  
- 9  —  ACQUISITION/DEVELOPMENT/INSTALLATION/IMPLEMENTATION CONTROLS

*For the content of the numbered topics and concepts above, refer to Exhibit 4-4.*
### INFORMATION TECHNOLOGY SECURITY TRAINING MATRIX — **Cell 2.2D**

<table>
<thead>
<tr>
<th>Training Area: <strong>Security Program — Management</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Functional Specialty: <strong>Implement &amp; Operate</strong></td>
</tr>
</tbody>
</table>

**Definition** — The implementation and use of organizational structures and processes for IT security program goal-setting, prioritizing, and related decision-making activities; these encompass such elements as organization-specific policies, guidelines, requirements, roles, responsibilities, and resource allocation.

**Behavioral Outcome** — Individuals who are responsible for the implementation and daily operations of an IT security program have a sufficient understanding of the appropriate program elements and requirements to be able to apply them in a manner which provides adequate and appropriate levels of protection for the organization’s IT resources.

**Knowledge Levels** —

1. Beginning — Identify, Understand, Apply
2. Intermediate — Interpret, Analyze, Decide
3. Advanced — Investigate, Approve, Direct

**Sample Learning Objectives** —

At the conclusion of this module, individuals will be able to:

1. Beginning — Apply organization-specific IT security program elements to the implementation of the program and identify areas of weakness.
2. Intermediate — Analyze patterns of non-compliance and take appropriate administrative or programmatic actions to minimize security risks.
3. Advanced — Direct the implementation of appropriate operational structures and processes to ensure an effective IT security program.

**Sample Job Functions** —

- Information Resources Management (IRM) Official, Senior
- Information Resources Manager
- IT Security Officer/Manager
- Network Administrator
- Program Manager
- System Administrator
- System Owner
### INFORMATION TECHNOLOGY SECURITY TRAINING MATRIX — Cell 2.2D

**Training Area:** Security Program — Management  
**Functional Specialty:** Implement & Operate

<table>
<thead>
<tr>
<th></th>
<th>IT SECURITY BODY OF KNOWLEDGE TOPICS AND CONCEPTS</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>LAWS AND REGULATIONS</td>
</tr>
<tr>
<td>2</td>
<td>IT SECURITY PROGRAM</td>
</tr>
<tr>
<td>3</td>
<td>SYSTEM ENVIRONMENT</td>
</tr>
<tr>
<td>4</td>
<td>SYSTEM INTERCONNECTION</td>
</tr>
<tr>
<td>5</td>
<td>INFORMATION SHARING</td>
</tr>
<tr>
<td>6</td>
<td>SENSITIVITY</td>
</tr>
<tr>
<td>7</td>
<td>RISK MANAGEMENT</td>
</tr>
<tr>
<td>8</td>
<td>MANAGEMENT CONTROLS</td>
</tr>
<tr>
<td>9</td>
<td>ACQUISITION/DEVELOPMENT/INSTALLATION/IMPLEMENTATION CONTROLS</td>
</tr>
<tr>
<td>10</td>
<td>OPERATIONAL CONTROLS</td>
</tr>
<tr>
<td>11</td>
<td>AWARENESS, TRAINING, AND EDUCATION CONTROLS</td>
</tr>
<tr>
<td>12</td>
<td>TECHNICAL CONTROLS</td>
</tr>
</tbody>
</table>

*For the content of the numbered topics and concepts above, refer to Exhibit 4-4.*
**INFORMATION TECHNOLOGY SECURITY TRAINING MATRIX — Cell 2.2E**

<table>
<thead>
<tr>
<th>Training Area: <strong>Security Program — Management</strong></th>
<th>Functional Specialty: <strong>Review &amp; Evaluate</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Definition</strong> — The implementation and use of organizational structures and processes for IT security program goal-setting, prioritizing, and related decision-making activities; these encompass such elements as organization-specific policies, guidelines, requirements, roles, responsibilities, and resource allocation.</td>
<td></td>
</tr>
<tr>
<td><strong>Behavioral Outcome</strong> — Individuals responsible for the review/evaluation of an IT security program have an adequate understanding of IT security laws, regulations, standards, guidelines, and the organizational environment to determine if the program adequately addresses all threats and areas of potential vulnerability.</td>
<td></td>
</tr>
<tr>
<td><strong>Knowledge Levels</strong> —</td>
<td></td>
</tr>
<tr>
<td>1. Beginning — Understand, Evaluate, Apply</td>
<td></td>
</tr>
<tr>
<td>2. Intermediate — Research, Compile, Interpret, Decide, Write</td>
<td></td>
</tr>
<tr>
<td>3. Advanced — Direct, Validate, Oversee</td>
<td></td>
</tr>
<tr>
<td><strong>Sample Learning Objectives</strong> —</td>
<td></td>
</tr>
<tr>
<td>At the conclusion of this module, individuals will be able to:</td>
<td></td>
</tr>
<tr>
<td>1. Beginning — Participate in the review of an organization’s IT security program and evaluate the extent to the program is being managed effectively.</td>
<td></td>
</tr>
<tr>
<td>2. Intermediate — Develop compliance findings and recommendations.</td>
<td></td>
</tr>
<tr>
<td>3. Advanced — Direct the review of the management of an organization’s IT security program, validate findings and recommendations, and establish follow-up monitoring for corrective actions.</td>
<td></td>
</tr>
<tr>
<td><strong>Sample Job Functions</strong> —</td>
<td></td>
</tr>
<tr>
<td>• Auditor, External</td>
<td></td>
</tr>
<tr>
<td>• Auditor, Internal</td>
<td></td>
</tr>
<tr>
<td>• Information Resources Management (IRM) Official, Senior</td>
<td></td>
</tr>
<tr>
<td>• IT Security Officer/Manager</td>
<td></td>
</tr>
<tr>
<td>IT SECURITY BODY OF KNOWLEDGE TOPICS AND CONCEPTS</td>
<td></td>
</tr>
<tr>
<td>-----------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>1. LAWS AND REGULATIONS</td>
<td></td>
</tr>
<tr>
<td>2. IT SECURITY PROGRAM</td>
<td></td>
</tr>
<tr>
<td>3. SYSTEM ENVIRONMENT</td>
<td></td>
</tr>
<tr>
<td>4. SYSTEM INTERCONNECTION</td>
<td></td>
</tr>
<tr>
<td>5. INFORMATION SHARING</td>
<td></td>
</tr>
<tr>
<td>6. SENSITIVITY</td>
<td></td>
</tr>
<tr>
<td>7. RISK MANAGEMENT</td>
<td></td>
</tr>
<tr>
<td>8. MANAGEMENT CONTROLS</td>
<td></td>
</tr>
<tr>
<td>9. ACQUISITION/DEVELOPMENT/INSTALLATION/</td>
<td></td>
</tr>
<tr>
<td>IMPLEMENTATION CONTROLS</td>
<td></td>
</tr>
<tr>
<td>10. OPERATIONAL CONTROLS</td>
<td></td>
</tr>
<tr>
<td>11. AWARENESS, TRAINING, AND EDUCATION CONTROLS</td>
<td></td>
</tr>
<tr>
<td>12. TECHNICAL CONTROLS</td>
<td></td>
</tr>
</tbody>
</table>

For the content of the numbered topics and concepts above, refer to Exhibit 4-4.
SECTION 4.2.3

TRAINING AREA:
SYSTEM LIFE CYCLE SECURITY
<table>
<thead>
<tr>
<th>INFORMATION TECHNOLOGY SECURITY TRAINING MATRIX — <strong>Cell 3.1A</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Training Area:</strong> System Life Cycle Security — Initiation</td>
</tr>
<tr>
<td><strong>Functional Specialty:</strong> Manage</td>
</tr>
<tr>
<td><strong>Definition</strong> — The system life cycle is a model for building</td>
</tr>
<tr>
<td><strong>Behavioral Outcome</strong> — Individuals with management</td>
</tr>
<tr>
<td><strong>Knowledge Levels</strong> —</td>
</tr>
<tr>
<td>1. Beginning — Understand, Know, Recognize</td>
</tr>
<tr>
<td>2. Intermediate — Identify, Assess, Decide</td>
</tr>
<tr>
<td>3. Advanced — Analyze, Approve, Direct</td>
</tr>
<tr>
<td><strong>Sample Job Functions</strong> —</td>
</tr>
<tr>
<td>• Information Resources Manager</td>
</tr>
<tr>
<td>• IT Security Officer/Manager</td>
</tr>
<tr>
<td>• Program Manager</td>
</tr>
<tr>
<td>• System Designer/Developer</td>
</tr>
<tr>
<td>• System Owner</td>
</tr>
<tr>
<td>INFORMATION TECHNOLOGY SECURITY TRAINING MATRIX — Cell 3.1A</td>
</tr>
<tr>
<td>-------------------------------------------------------------</td>
</tr>
<tr>
<td>Training Area: System Life Cycle Security — Initiation</td>
</tr>
<tr>
<td>Functional Specialty: Manage</td>
</tr>
</tbody>
</table>

**IT SECURITY BODY OF KNOWLEDGE TOPICS AND CONCEPTS**

- 2  —  IT SECURITY PROGRAM
- 5  —  INFORMATION SHARING
- 6  —  SENSITIVITY
- 8  —  MANAGEMENT CONTROLS
- 9  —  ACQUISITION/DEVELOPMENT/INSTALLATION/IMPLEMENTATION CONTROLS

*For the content of the numbered topics and concepts above, refer to Exhibit 4-4.*
<table>
<thead>
<tr>
<th>INFORMATION TECHNOLOGY SECURITY TRAINING MATRIX — <strong>Cell 3.1B</strong></th>
</tr>
</thead>
</table>
| **Training Area:** System Life Cycle Security — Initiation  
**Functional Specialty:** Acquire |
| **Definition** — The system life cycle is a model for building and operating an IT system from its initial inception to its termination and disposal of assets. The model includes six phases: Initiation, Development, Test and Evaluation, Implementation, Operations, and Termination. Life cycle security is the ensemble of processes and procedures which ensures data confidentiality, as needed, as well as data and system integrity, and availability.  
The initiation phase is the series of steps followed to ensure that security requirements are considered and resolved as new information systems and technologies are planned. |
| **Behavioral Outcome** — Individuals with acquisition responsibilities are able to analyze and develop acquisition documents and/or provide guidance which ensures that functional IT security requirements are incorporated. |
| **Knowledge Levels** —  
1. Beginning — Identify, Locate, Understand  
2. Intermediate — Develop, Research, Write  
3. Advanced — Analyze, Evaluate, Approve |
| **Sample Learning Objectives** —  
At the conclusion of this module, individuals will be able to:  
1. Beginning — Identify general and system-specific IT security specifications which pertain to a particular system acquisition being planned.  
2. Intermediate — Develop security-related portions of acquisition documents.  
3. Advanced — Ensure that security-related portions of the system acquisition documents meet all identified security needs. |
| **Sample Job Functions** —  
- Contracting Officer  
- Contracting Officer’s Technical Representative (COTR)  
- IT Security Officer/Manager  
- System Designer/Developer  
- System Owner |
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>IT SECURITY BODY OF KNOWLEDGE TOPICS AND CONCEPTS</strong></td>
<td></td>
</tr>
<tr>
<td>• 2 — IT SECURITY PROGRAM</td>
<td></td>
</tr>
<tr>
<td>• 3 — SYSTEM ENVIRONMENT</td>
<td></td>
</tr>
<tr>
<td>• 4 — SYSTEM INTERCONNECTION</td>
<td></td>
</tr>
<tr>
<td>• 5 — INFORMATION SHARING</td>
<td></td>
</tr>
<tr>
<td>• 6 — SENSITIVITY</td>
<td></td>
</tr>
<tr>
<td>• 9 — ACQUISITION/DEVELOPMENT/INSTALLATION/</td>
<td></td>
</tr>
<tr>
<td>IMPLEMENTATION CONTROLS</td>
<td></td>
</tr>
<tr>
<td>• 10 — OPERATIONAL CONTROLS</td>
<td></td>
</tr>
<tr>
<td>• 12 — TECHNICAL CONTROLS</td>
<td></td>
</tr>
</tbody>
</table>

*For the content of the numbered topics and concepts above, refer to Exhibit 4-4.*
<table>
<thead>
<tr>
<th>INFORMATION TECHNOLOGY SECURITY TRAINING MATRIX — <strong>Cell 3.1C</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Training Area:</strong> <strong>System Life Cycle Security — Initiation</strong></td>
</tr>
<tr>
<td><strong>Functional Specialty:</strong> <strong>Design &amp; Develop</strong></td>
</tr>
<tr>
<td><strong>Definition</strong> — The system life cycle is a model for building</td>
</tr>
<tr>
<td>assets. The model includes six phases:</td>
</tr>
<tr>
<td>Initiation, Development, Test and Evaluation,</td>
</tr>
<tr>
<td>Implementation, Operations, and Termination.</td>
</tr>
<tr>
<td>Life cycle security is the ensemble of</td>
</tr>
<tr>
<td>processes and procedures which ensures data</td>
</tr>
<tr>
<td>confidentiality, as needed, as well as data</td>
</tr>
<tr>
<td>and system integrity, and availability.</td>
</tr>
<tr>
<td>The initiation phase is the series of steps</td>
</tr>
<tr>
<td>followed to ensure that security requirements</td>
</tr>
<tr>
<td>are considered and resolved as new information</td>
</tr>
<tr>
<td>systems and technologies are planned.</td>
</tr>
<tr>
<td><strong>Behavioral Outcome</strong> — Individuals responsible for the</td>
</tr>
<tr>
<td>design and development of IT systems are able</td>
</tr>
<tr>
<td>to translate IT security requirements into</td>
</tr>
<tr>
<td>system-level security specifications.</td>
</tr>
<tr>
<td><strong>Knowledge Levels</strong> —</td>
</tr>
<tr>
<td>1. Beginning — Identify, Define, Participate</td>
</tr>
<tr>
<td>2. Intermediate — Understand, Interpret, Translate</td>
</tr>
<tr>
<td>3. Advanced — Analyze, Determine, Approve</td>
</tr>
<tr>
<td><strong>Sample Learning Objectives</strong> —</td>
</tr>
<tr>
<td>At the conclusion of this module, individuals will be able to:</td>
</tr>
<tr>
<td>1. Beginning — Identify areas where specific IT security</td>
</tr>
<tr>
<td>countermeasures are required and participate</td>
</tr>
<tr>
<td>in the development of security strategies.</td>
</tr>
<tr>
<td>2. Intermediate — Translate IT security strategies into</td>
</tr>
<tr>
<td>initial security specifications for the</td>
</tr>
<tr>
<td>planned system.</td>
</tr>
<tr>
<td>3. Advanced — Approve IT security specifications for inclusion</td>
</tr>
<tr>
<td>in the formal system baseline.</td>
</tr>
<tr>
<td><strong>Sample Job Functions</strong> —</td>
</tr>
<tr>
<td>• IT Security Officer/Manager</td>
</tr>
<tr>
<td>• Program Manager</td>
</tr>
<tr>
<td>• System Designer/Developer</td>
</tr>
<tr>
<td>• System Owner</td>
</tr>
</tbody>
</table>
### INFORMATION TECHNOLOGY SECURITY TRAINING MATRIX — **Cell 3.1C**

**Training Area:** System Life Cycle Security — Initiation  
**Functional Specialty:** Design & Develop

#### IT SECURITY BODY OF KNOWLEDGE TOPICS AND CONCEPTS

- 2 — IT SECURITY PROGRAM  
- 3 — SYSTEM ENVIRONMENT  
- 4 — SYSTEM INTERCONNECTION  
- 5 — INFORMATION SHARING  
- 6 — SENSITIVITY  
- 9 — ACQUISITION/DEVELOPMENT/INSTALLATION/IMPLEMENTATION CONTROLS

*For the content of the numbered topics and concepts above, refer to Exhibit 4-4.*
<table>
<thead>
<tr>
<th>INFORMATION TECHNOLOGY SECURITY TRAINING MATRIX — <strong>Cell 3.1E</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Training Area:</strong> System Life Cycle Security — Initiation</td>
</tr>
<tr>
<td><strong>Functional Specialty:</strong> Review &amp; Evaluate</td>
</tr>
<tr>
<td><strong>Definition</strong> — The system life cycle is a model for building and operating an IT system from its initial inception to its termination and disposal of assets. The model includes six phases: Initiation, Development, Test and Evaluation, Implementation, Operations, and Termination. Life cycle security is the ensemble of processes and procedures which ensures data confidentiality, as needed, as well as data and system integrity, and availability.</td>
</tr>
<tr>
<td>The initiation phase is the series of steps followed to ensure that security requirements are considered and resolved as new information systems and technologies are planned.</td>
</tr>
<tr>
<td><strong>Behavioral Outcome</strong> — Individuals are able to evaluate planning documents associated with a particular system to ensure that appropriate IT security requirements have been considered and incorporated.</td>
</tr>
<tr>
<td><strong>Knowledge Levels</strong> —</td>
</tr>
<tr>
<td>1. Beginning — Understand, Participate, Assess</td>
</tr>
<tr>
<td>2. Intermediate — Conduct, Research, Interpret</td>
</tr>
<tr>
<td>3. Advanced — Verify, Analyze, Recommend</td>
</tr>
<tr>
<td><strong>Sample Learning Objectives</strong> —</td>
</tr>
<tr>
<td>At the conclusion of this module, individuals will be able to:</td>
</tr>
<tr>
<td>1. Beginning — Participate in the evaluation of functional IT security requirements for a system.</td>
</tr>
<tr>
<td>2. Intermediate — Conduct the review and evaluation of functional IT security requirements for a system.</td>
</tr>
<tr>
<td>3. Advanced — Verify that the security requirements for a system are appropriately incorporated into the system design.</td>
</tr>
<tr>
<td><strong>Sample Job Functions</strong> —</td>
</tr>
<tr>
<td>• Auditor, External</td>
</tr>
<tr>
<td>• Auditor, Internal</td>
</tr>
<tr>
<td>• Information Resources Manager</td>
</tr>
<tr>
<td>• IT Security Officer/Manager</td>
</tr>
<tr>
<td>• System Owner</td>
</tr>
</tbody>
</table>
## INFORMATION TECHNOLOGY SECURITY TRAINING MATRIX — Cell 3.1E

<table>
<thead>
<tr>
<th>Training Area: <strong>Laws &amp; Regulations</strong></th>
<th>Functional Specialty: <strong>Review &amp; Evaluate</strong></th>
</tr>
</thead>
</table>

### IT SECURITY BODY OF KNOWLEDGE TOPICS AND CONCEPTS

- 2 — IT SECURITY PROGRAM
- 3 — SYSTEM ENVIRONMENT
- 4 — SYSTEM INTERCONNECTION
- 5 — INFORMATION SHARING
- 6 — SENSITIVITY
- 7 — RISK MANAGEMENT
- 8 — MANAGEMENT CONTROLS
- 9 — ACQUISITION/DEVELOPMENT/INSTALLATION/IMPLEMENTATION CONTROLS
- 10 — OPERATIONAL CONTROLS
- 11 — AWARENESS, TRAINING, AND EDUCATION CONTROLS
- 12 — TECHNICAL CONTROLS

For the content of the numbered topics and concepts above, refer to **Exhibit 4-4**.
### INFORMATION TECHNOLOGY SECURITY TRAINING MATRIX — **Cell 3.1F**

**Training Area:** System Life Cycle Security — Initiation  
**Functional Specialty:** Use

#### Definition
The system life cycle is a model for building and operating an IT system from its initial inception to its termination and disposal of assets. The model includes six phases: Initiation, Development, Test and Evaluation, Implementation, Operations, and Termination. Life cycle security is the ensemble of processes and procedures which ensures data confidentiality, as needed, as well as data and system integrity, and availability.

The initiation phase is the series of steps followed to ensure that security requirements are considered and resolved as new information systems and technologies are planned.

#### Behavioral Outcome
Potential users are able to participate in needs analyses and understand the various points of view involved in setting the balance between IT security controls and system efficiency.

#### Knowledge Levels
1. **Beginning** — Understand, Identify
2. **Intermediate/Advanced** — Know, Analyze, Participate, Suggest

#### Sample Learning Objectives
At the conclusion of this module, individuals will be able to:

1. **Beginning** — Participate in the identification of system confidentiality, integrity, and availability requirements in relation to user needs and risk management.
2. **Intermediate/Advanced** — Participate in the analysis and selection of security alternatives.

#### Sample Job Functions
- IT Security Officer/Manager
- System Owner
- User
<table>
<thead>
<tr>
<th>INFORMATION TECHNOLOGY SECURITY TRAINING MATRIX — Cell 3.1F</th>
</tr>
</thead>
<tbody>
<tr>
<td>Training Area: <strong>Laws &amp; Regulations</strong></td>
</tr>
<tr>
<td>Functional Specialty: <strong>Use</strong></td>
</tr>
</tbody>
</table>

**IT SECURITY BODY OF KNOWLEDGE TOPICS AND CONCEPTS**

- **2** — IT SECURITY PROGRAM
- **6** — SENSITIVITY
- **7** — RISK MANAGEMENT

*For the content of the numbered topics and concepts above, refer to Exhibit 4-4.*
### INFORMATION TECHNOLOGY SECURITY TRAINING MATRIX — **Cell 3.2A**

**Training Area:** System Life Cycle Security — Development  
**Functional Specialty:** Manage

#### Definition —

The system life cycle is a model for building and operating an IT system from its initial inception to its termination and disposal of assets. The model includes six phases: Initiation, Development, Test and Evaluation, Implementation, Operations, and Termination. Life cycle security is the ensemble of processes and procedures which ensures data confidentiality, as needed, as well as data and system integrity, and availability.

The development phase is the series of steps followed to ensure that security requirements are considered, resolved, and incorporated as information systems and technologies are developed or changed.

#### Behavioral Outcome —

Individuals with management responsibilities are able to ensure that the formal developmental baseline includes approved security requirements and that security-related features are installed, clearly identified, and documented.

#### Knowledge Levels —

1. **Beginning** — Understand, Know, Apply  
2. **Intermediate** — Identify, Review, Decide  
3. **Advanced** — Evaluate, Analyze, Approve

#### Sample Learning Objectives —

At the conclusion of this module, individuals will be able to:

1. **Beginning** — Understand the relationship between planned security safeguards and the features being installed on the system under development. Provide input on security concerns during system development efforts.

2. **Intermediate** — Review the selected security safeguards to determine if security concerns identified in the approved plan have been fully addressed.

3. **Advanced** — Evaluate and approve development efforts to ensure that baseline security safeguards are appropriately installed for the system being developed or modified.

#### Sample Job Functions —

- Information Resources Manager  
- IT Security Officer/Manager  
- System Designer/Developer  
- System Owner
**INFORMATION TECHNOLOGY SECURITY TRAINING MATRIX — Cell 3.2A**

Training Area: **System Life Cycle Security — Development**  
Functional Specialty: **Manage**

<table>
<thead>
<tr>
<th>IT SECURITY BODY OF KNOWLEDGE TOPICS AND CONCEPTS</th>
</tr>
</thead>
<tbody>
<tr>
<td>• 4    —   SYSTEM INTERCONNECTION</td>
</tr>
<tr>
<td>• 5    —   INFORMATION SHARING</td>
</tr>
<tr>
<td>• 6    —   SENSITIVITY</td>
</tr>
<tr>
<td>• 7    —   RISK MANAGEMENT</td>
</tr>
<tr>
<td>• 8    —   MANAGEMENT CONTROLS</td>
</tr>
<tr>
<td>• 9    —   ACQUISITION/DEVELOPMENT/INSTALLATION/IMPLEMENTATION CONTROLS</td>
</tr>
</tbody>
</table>

*For the content of the numbered topics and concepts above, refer to Exhibit 4-4.*
### INFORMATION TECHNOLOGY SECURITY TRAINING MATRIX — **Cell 3.2B**

**Training Area:** System Life Cycle Security — Development  
**Functional Specialty:** Acquire

| Definition | The system life cycle is a model for building and operating an IT system from its initial inception to its termination and disposal of assets. The model includes six phases: Initiation, Development, Test and Evaluation, Implementation, Operations, and Termination. Life cycle security is the ensemble of processes and procedures which ensures data confidentiality, as needed, as well as data and system integrity, and availability.  

The development phase is the series of steps followed to ensure that security requirements are considered, resolved, and incorporated as information systems and technologies are developed or changed. |
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Behavioral Outcome</td>
<td>Individuals with acquisition responsibilities are able to monitor procurement actions to ensure that IT security requirements are satisfied.</td>
</tr>
<tr>
<td>Knowledge Levels</td>
<td></td>
</tr>
</tbody>
</table>
1. Beginning — Identify, Know, Apply  
2. Intermediate/Advanced — Evaluate, Analyze, Interpret |
| Sample Learning Objectives | At the conclusion of this module, individuals will be able to:  
1. Beginning — Ensure that IT security requirements are appropriately identified in acquisition documents.  
2. Intermediate/Advanced — Evaluate the presence and adequacy of security measures proposed or provided in response to requirements contained in acquisition documents. |
| Sample Job Functions |  
- Contracting Officer  
- Contracting Officer’s Technical Representative (COTR)  
- IT Security Officer/Manager  
- Source Selection Board Member  
- System Owner |
<table>
<thead>
<tr>
<th>INFORMATION TECHNOLOGY SECURITY TRAINING MATRIX — Cell 3.2B</th>
</tr>
</thead>
<tbody>
<tr>
<td>Training Area: <strong>System Life Cycle Security — Development</strong></td>
</tr>
<tr>
<td>Functional Specialty: <strong>Acquire</strong></td>
</tr>
</tbody>
</table>

**IT SECURITY BODY OF KNOWLEDGE TOPICS AND CONCEPTS**

- 9 — ACQUISITION/DEVELOPMENT/INSTALLATION/IMPLEMENTATION CONTROLS

*For the content of the numbered topics and concepts above, refer to Exhibit 4-4.*
### INFORMATION TECHNOLOGY SECURITY TRAINING MATRIX — **Cell 3.2C**

<table>
<thead>
<tr>
<th>Training Area: System Life Cycle Security — Development</th>
</tr>
</thead>
<tbody>
<tr>
<td>Functional Specialty: Design &amp; Develop</td>
</tr>
</tbody>
</table>

**Definition** — The system life cycle is a model for building and operating an IT system from its initial inception to its termination and disposal of assets. The model includes six phases: Initiation, Development, Test and Evaluation, Implementation, Operations, and Termination. Life cycle security is the ensemble of processes and procedures which ensures data confidentiality, as needed, as well as data and system integrity, and availability.

The development phase is the series of steps followed to ensure that security requirements are considered, resolved, and incorporated as information systems and technologies are developed or changed.

**Behavioral Outcome** — Individuals responsible for system design, development or modification are able to use baseline IT security requirements to select and install appropriate safeguards.

**Knowledge Levels** —

1. Beginning — Know, Construct, Apply
2. Intermediate — Identify, Recommend, Interpret
3. Advanced — Determine, Select, Approve

**Sample Learning Objectives** —

At the conclusion of this module, individuals will be able to:

1. Beginning — Participate in the construction of the IT system in accordance with the formal design specifications: developing manual procedures, using off-the-shelf hardware/software components, writing program code, customizing hardware components, and/or using other IT capabilities.

2. Intermediate — Identify and recommend alternative safeguards that will satisfy baseline security specifications.

3. Advanced — Review recommendations and select appropriate safeguards for implementation.

**Sample Job Functions** —

- Freedom of Information Act Official
- IT Security Officer/Manager
- System Designer/Developer
- Programmer/Systems Analyst
- Records Management Official
- Privacy Act Official
INFORMATION TECHNOLOGY SECURITY TRAINING MATRIX — **Cell 3.2C**

<table>
<thead>
<tr>
<th>Training Area: System Life Cycle Security — Development</th>
</tr>
</thead>
<tbody>
<tr>
<td>Functional Specialty: Design &amp; Develop</td>
</tr>
</tbody>
</table>

## IT SECURITY BODY OF KNOWLEDGE TOPICS AND CONCEPTS

- 2 — IT SECURITY PROGRAM
- 3 — SYSTEM ENVIRONMENT
- 4 — SYSTEM INTERCONNECTION
- 5 — INFORMATION SHARING
- 6 — SENSITIVITY
- 7 — RISK MANAGEMENT
- 9 — ACQUISITION/DEVELOPMENT/INSTALLATION/IMPLEMENTATION CONTROLS

*For the content of the numbered topics and concepts above, refer to Exhibit 4-4.*
<table>
<thead>
<tr>
<th>INFORMATION TECHNOLOGY SECURITY TRAINING MATRIX — <strong>Cell 3.2D</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Training Area:</strong> System Life Cycle Security — Development</td>
</tr>
<tr>
<td><strong>Functional Specialty:</strong> Implement &amp; Operate</td>
</tr>
<tr>
<td><strong>Definition</strong> — The system life cycle is a model for building and operating an IT system from its initial inception to its termination and disposal of assets. The model includes six phases: Initiation, Development, Test and Evaluation, Implementation, Operations, and Termination. Life cycle security is the ensemble of processes and procedures which ensures data confidentiality, as needed, as well as data and system integrity, and availability.</td>
</tr>
<tr>
<td>The development phase is the series of steps followed to ensure that security requirements are considered, resolved, and incorporated as information systems and technologies are developed or changed.</td>
</tr>
<tr>
<td><strong>Behavioral Outcome</strong> — Individuals responsible for system implementation or operation are able to assemble, integrate, and install systems so that the functionality and effectiveness of safeguards can be tested and evaluated.</td>
</tr>
<tr>
<td><strong>Knowledge Levels</strong> —</td>
</tr>
<tr>
<td>1. Beginning — Install, Operate, Understand</td>
</tr>
<tr>
<td>2. Intermediate — Analyze, Approve, Recommend</td>
</tr>
<tr>
<td>3. Advanced — Direct, Require, Ensure</td>
</tr>
<tr>
<td><strong>Sample Learning Objectives</strong> —</td>
</tr>
<tr>
<td>At the conclusion of this module, individuals will be able to:</td>
</tr>
<tr>
<td>1. Beginning — Install and operate the IT systems in a test configuration in a manner that does not alter the program code or compromise security safeguards.</td>
</tr>
<tr>
<td>2. Intermediate — Analyze system performance for potential security problems (e.g., failure to update access control tables, corrupted data).</td>
</tr>
<tr>
<td>3. Advanced — Provide direction to system developers regarding correction of security problems identified during testing.</td>
</tr>
<tr>
<td><strong>Sample Job Functions</strong> —</td>
</tr>
<tr>
<td>• Data Center Manager</td>
</tr>
<tr>
<td>• Database Administrator</td>
</tr>
<tr>
<td>• IT Security Officer/Manager</td>
</tr>
<tr>
<td>• Network Administrator</td>
</tr>
<tr>
<td>• System Administrator</td>
</tr>
<tr>
<td>• System Designer/Developer</td>
</tr>
<tr>
<td>• System Operations Personnel</td>
</tr>
<tr>
<td>• Technical Support Personnel</td>
</tr>
<tr>
<td>Training Area: System Life Cycle Security — Development</td>
</tr>
<tr>
<td>--------------------------------------------------------</td>
</tr>
<tr>
<td>Functional Specialty: Implement &amp; Operate</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>IT SECURITY BODY OF KNOWLEDGE TOPICS AND CONCEPTS</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>• 3 — SYSTEM ENVIRONMENT</td>
</tr>
<tr>
<td>• 4 — SYSTEM INTERCONNECTION</td>
</tr>
<tr>
<td>• 5 — INFORMATION SHARING</td>
</tr>
<tr>
<td>• 8 — MANAGEMENT CONTROLS</td>
</tr>
<tr>
<td>• 9 — ACQUISITION/DEVELOPMENT/INSTALLATION/IMPLEMENTATION CONTROLS</td>
</tr>
<tr>
<td>• 10 — OPERATIONAL CONTROLS</td>
</tr>
<tr>
<td>• 12 — TECHNICAL CONTROLS</td>
</tr>
</tbody>
</table>

*For the content of the numbered topics and concepts above, refer to Exhibit 4-4.*
**INFORMATION TECHNOLOGY SECURITY TRAINING MATRIX — Cell 3.2E**

<table>
<thead>
<tr>
<th>Training Area: System Life Cycle Security — Development</th>
</tr>
</thead>
<tbody>
<tr>
<td>Functional Specialty: <strong>Review &amp; Evaluate</strong></td>
</tr>
</tbody>
</table>

**Definition** — The system life cycle is a model for building and operating an IT system from its initial inception to its termination and disposal of assets. The model includes six phases: Initiation, Development, Test and Evaluation, Implementation, Operations, and Termination. Life cycle security is the ensemble of processes and procedures which ensures data confidentiality, as needed, as well as data and system integrity, and availability.

The development phase is the series of steps followed to ensure that security requirements are considered, resolved, and incorporated as information systems and technologies are developed or changed.

**Behavioral Outcome** — Individuals responsible for review and evaluation are able to examine development efforts at specified milestones to ensure that approved safeguards are in place and documented.

**Knowledge Levels** —

1. Beginning — Know, Review, Evaluate
2. Intermediate/Advanced — Analyze, Recommend, Approve

**Sample Learning Objectives** —

At the conclusion of this module, individuals will be able to:

1. Beginning — Review IT system development documents for inclusion of appropriate safeguards.

2. Intermediate — Review and evaluate IT system development documents to ensure that system safeguards, as a whole, result in an acceptable level of risk.

3. Advanced — Evaluate configuration controls, review development of security test plans and procedures, and ensure that security requirements are documented and comply with the formal design specification.

**Sample Job Functions** —

- Auditor, External
- Auditor, Internal
- Certification Reviewer
- Designated Approving Authority (DAA)
- IT Security Officer/Manager
- Program Manager
- System Owner
### INFORMATION TECHNOLOGY SECURITY TRAINING MATRIX — Cell 3.2E

<table>
<thead>
<tr>
<th>Training Area: System Life Cycle Security — Development</th>
</tr>
</thead>
<tbody>
<tr>
<td>Functional Specialty: Review &amp; Evaluate</td>
</tr>
</tbody>
</table>

**IT SECURITY BODY OF KNOWLEDGE TOPICS AND CONCEPTS**

- **7** — RISK MANAGEMENT
- **8** — MANAGEMENT CONTROLS
- **9** — ACQUISITION/DEVELOPMENT/INSTALLATION/IMPLEMENTATION CONTROLS
- **10** — OPERATIONAL CONTROLS
- **12** — TECHNICAL CONTROLS

*For the content of the numbered topics and concepts above, refer to Exhibit 4-4.*
### INFORMATION TECHNOLOGY SECURITY TRAINING MATRIX — **Cell 3.2F**

| Training Area: **System Life Cycle Security — Development**  
| Functional Specialty: **Use**  

**Definition** —  The system life cycle is a model for building and operating an IT system from its initial inception to its termination and disposal of assets. The model includes six phases: Initiation, Development, Test and Evaluation, Implementation, Operations, and Termination. Life cycle security is the ensemble of processes and procedures which ensures data confidentiality, as needed, as well as data and system integrity, and availability.

The development phase is the series of steps followed to ensure that security requirements are considered, resolved, and incorporated as information systems and technologies are developed or changed.

**Behavioral Outcome** —  Potential users are able to provide input to system development efforts to ensure that IT security safeguards are as transparent to the user as feasible and are balanced with ease of use.

**Knowledge Levels** —

1. Beginning/Intermediate/Advanced — Understand, Know, Apply

**Sample Learning Objectives** —

At the conclusion of this module, individuals will be able to:

1. Beginning/Intermediate/Advanced — Appreciate the balance between operational efficiency, integrity, and availability for the system under development.

**Sample Job Functions** —

- IT Security Officer/Manager
- User
<table>
<thead>
<tr>
<th>INFORMATION TECHNOLOGY SECURITY TRAINING MATRIX — <strong>Cell 3.2F</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Training Area:</strong> System Life Cycle Security — Development</td>
</tr>
<tr>
<td><strong>Functional Specialty:</strong> <strong>Use</strong></td>
</tr>
</tbody>
</table>

**IT SECURITY BODY OF KNOWLEDGE TOPICS AND CONCEPTS**

- **6** — SENSITIVITY
- **8** — MANAGEMENT CONTROLS

*For the content of the numbered topics and concepts above, refer to Exhibit 4-4.*
INFORMATION TECHNOLOGY SECURITY TRAINING MATRIX — Cell 3.3C

Training Area: **System Life Cycle Security — Test & Evaluate**  
Functional Specialty: **Design & Develop**

**Definition** — The system life cycle is a model for building and operating an IT system from its initial inception to its termination and disposal of assets. The model includes six phases: Initiation, Development, Test and Evaluation, Implementation, Operations, and Termination. Life cycle security is the ensemble of processes and procedures which ensures data confidentiality, as needed, as well as data and system integrity, and availability.

The test and evaluation phase is the series of steps followed to ensure that the design and construction of a new or modified information system or technology has successfully incorporated appropriate security safeguards.

**Behavioral Outcome** — Individuals are able to design tests to evaluate the adequacy of security safeguards in IT systems.

**Knowledge Levels** —

1. Beginning — Know, Design, Write  
2. Intermediate — Analyze, Design, Develop  
3. Advanced — Interpret, Evaluate, Approve

**Sample Learning Objectives** —

At the conclusion of this module, individuals will be able to:

1. Beginning — Design and develop tests for security safeguard performance under normal operating circumstances and workload levels.

2. Intermediate — Design and develop tests for security safeguard performance under abnormal, unusual, improbable, and/or illegal circumstances.

3. Advanced — Ensure that all security-related elements (e.g., system components, documentation) will be effectively tested.

**Sample Job Functions** —

- IT Security Officer/Manager  
- Programmer/Systems Analyst  
- System Designer/Developer
## INFORMATION TECHNOLOGY SECURITY TRAINING MATRIX — **Cell 3.3C**

<table>
<thead>
<tr>
<th>Training Area: <strong>System Life Cycle Security — Test &amp; Evaluate</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Functional Specialty: <strong>Design &amp; Develop</strong></td>
</tr>
</tbody>
</table>

### IT SECURITY BODY OF KNOWLEDGE TOPICS AND CONCEPTS

- **9** — ACQUISITION/DEVELOPMENT/INSTALLATION/IMPLEMENTATION CONTROLS
- **10** — OPERATIONAL CONTROLS
- **12** — TECHNICAL CONTROLS

For the content of the numbered topics and concepts above, refer to **Exhibit 4-4**.
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Definition</strong> — The system life cycle is a model for building and operating an IT system from its initial inception to its termination and disposal of assets. The model includes six phases: Initiation, Development, Test and Evaluation, Implementation, Operations, and Termination. Life cycle security is the ensemble of processes and procedures which ensures data confidentiality, as needed, as well as data and system integrity, and availability.</td>
<td></td>
</tr>
<tr>
<td>The test and evaluation phase is the series of steps followed to ensure that the design and construction of a new or modified information system or technology has successfully incorporated appropriate security safeguards.</td>
<td></td>
</tr>
<tr>
<td><strong>Behavioral Outcome</strong> — Individuals responsible for system implementation or operation are able to conduct tests of the effectiveness of security safeguards in the integrated system.</td>
<td></td>
</tr>
<tr>
<td><strong>Knowledge Levels</strong> —</td>
<td></td>
</tr>
<tr>
<td>1. Beginning — Conduct, Apply, Recognize, Document</td>
<td></td>
</tr>
<tr>
<td>2. Intermediate — Assess, Understand, Interpret</td>
<td></td>
</tr>
<tr>
<td>3. Advanced — Evaluate, Decide, Recommend</td>
<td></td>
</tr>
<tr>
<td><strong>Sample Learning Objectives</strong> —</td>
<td></td>
</tr>
<tr>
<td>At the conclusion of this module, individuals will be able to:</td>
<td></td>
</tr>
<tr>
<td>1. Beginning — Conduct tests of security safeguards in accordance with the established test plan and procedures.</td>
<td></td>
</tr>
<tr>
<td>2. Intermediate — Assess the performance of security controls (to include hardware, software, firmware, and telecommunications as appropriate) to ensure that the residual risk is within an acceptable range.</td>
<td></td>
</tr>
<tr>
<td>3. Advanced — Evaluate functional operation and performance in light of test results and make recommendations regarding certification and accreditation.</td>
<td></td>
</tr>
<tr>
<td><strong>Sample Job Functions</strong> —</td>
<td></td>
</tr>
<tr>
<td>• Certification Reviewer</td>
<td></td>
</tr>
<tr>
<td>• Database Administrator</td>
<td></td>
</tr>
<tr>
<td>• Designated Approving Authority</td>
<td></td>
</tr>
<tr>
<td>• IT Security Officer/Manager</td>
<td></td>
</tr>
<tr>
<td>• Network Administrator</td>
<td></td>
</tr>
<tr>
<td>• Programmer/Systems Analyst</td>
<td></td>
</tr>
<tr>
<td>• System Administrator</td>
<td></td>
</tr>
<tr>
<td>• System Operations Personnel</td>
<td></td>
</tr>
<tr>
<td>INFORMATION TECHNOLOGY SECURITY TRAINING MATRIX — Cell 3.3D</td>
<td></td>
</tr>
<tr>
<td>-------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>Training Area: <strong>System Life Cycle Security — Test &amp; Evaluate</strong></td>
<td></td>
</tr>
<tr>
<td>Functional Specialty: <strong>Implement &amp; Operate</strong></td>
<td></td>
</tr>
</tbody>
</table>

**IT SECURITY BODY OF KNOWLEDGE TOPICS AND CONCEPTS**

- 3 — SYSTEM ENVIRONMENT
- 4 — SYSTEM INTERCONNECTION
- 5 — INFORMATION SHARING
- 7 — RISK MANAGEMENT
- 8 — MANAGEMENT CONTROLS
- 9 — ACQUISITION/DEVELOPMENT/INSTALLATION/IMPLEMENTATION CONTROLS
- 10 — OPERATIONAL CONTROLS
- 12 — TECHNICAL CONTROLS

*For the content of the numbered topics and concepts above, refer to Exhibit 4-4.*
### INFORMATION TECHNOLOGY SECURITY TRAINING MATRIX — Cell 3.3E

<table>
<thead>
<tr>
<th>Training Area: System Life Cycle Security — Test &amp; Evaluate</th>
</tr>
</thead>
<tbody>
<tr>
<td>Functional Specialty: Review &amp; Evaluate</td>
</tr>
</tbody>
</table>

**Definition** — The system life cycle is a model for building and operating an IT system from its initial inception to its termination and disposal of assets. The model includes six phases: Initiation, Development, Test and Evaluation, Implementation, Operations, and Termination. Life cycle security is the ensemble of processes and procedures which ensures data confidentiality, as needed, as well as data and system integrity, and availability.

The test and evaluation phase is the series of steps followed to ensure that the design and construction of a new or modified information system or technology has successfully incorporated appropriate security safeguards.

**Behavioral Outcome** — Individuals are able to evaluate the appropriateness of test methodologies, and conduct independent tests and evaluations to ensure that adequate and appropriate safeguards are in place, effective, and documented; and to prepare certification/accreditation documentation.

**Knowledge Levels** —

1. Beginning — Know, Perform, Apply
2. Intermediate/Advanced — Evaluate, Interpret, Decide

**Sample Learning Objectives** —

At the conclusion of this module, individuals will be able to:

1. Beginning — Participate in or perform independent tests and document results.

2. Intermediate/Advanced — Evaluate configuration controls, review security test plans and procedures, ensure that documented security requirements are tested and comply with formal design specifications, and prepare certification/accreditation documentation.

**Sample Job Functions** —

- Auditor, External
- Auditor, Internal
- Certification Reviewer
- Designated Approving Authority (DAA)
- Information Resources Management (IRM) Official, Senior
- IT Security Officer/Manager
- System Owner
### INFORMATION TECHNOLOGY SECURITY TRAINING MATRIX — **Cell 3.3E**

**Training Area:** System Life Cycle Security — Test & Evaluate  
**Functional Specialty:** Review & Evaluate

#### IT SECURITY BODY OF KNOWLEDGE TOPICS AND CONCEPTS

- **3** — SYSTEM ENVIRONMENT  
- **4** — SYSTEM INTERCONNECTION  
- **5** — INFORMATION SHARING  
- **8** — MANAGEMENT CONTROLS  
- **9** — ACQUISITION/DEVELOPMENT/INSTALLATION/IMPLEMENTATION CONTROLS  
- **10** — OPERATIONAL CONTROLS  
- **12** — TECHNICAL CONTROLS

*For the content of the numbered topics and concepts above, refer to *Exhibit 4-4*.  

---

*Chapter 4. Training Development Methodology 122*
Training Area: **System Life Cycle Security — Test & Evaluate**  
Functional Specialty: **Use**

**Definition** — The system life cycle is a model for building and operating an IT system from its initial inception to its termination and disposal of assets. The model includes six phases: Initiation, Development, Test and Evaluation, Implementation, Operations, and Termination. Life cycle security is the ensemble of processes and procedures which ensures data confidentiality, as needed, as well as data and system integrity, and availability.

The test and evaluation phase is the series of steps followed to ensure that the design and construction of a new or modified information system or technology has successfully incorporated appropriate security safeguards.

**Behavioral Outcome** — Users are able to participate in acceptance tests and evaluate the impact of security safeguards on the operational environment.

**Knowledge Levels** —

1. Beginning/Intermediate/Advanced — Develop, Evaluate, Decide

**Sample Learning Objectives** —

At the conclusion of this module, individuals will be able to:

1. Beginning/Intermediate/Advanced — Develop test scenarios for use in acceptance testing of security countermeasures in a normal work environment. Participate in the evaluation of test results to determine the impact of security safeguards on user operations.

**Sample Job Functions** —

- IT Security Officer/Manager
- System Owner
- User
### INFORMATION TECHNOLOGY SECURITY TRAINING MATRIX — Cell 3.3F

| Training Area: System Life Cycle Security — Test & Evaluate |
| Functional Specialty: Use |

**IT SECURITY BODY OF KNOWLEDGE TOPICS AND CONCEPTS**

- 8 — MANAGEMENT CONTROLS
- 10 — OPERATIONAL CONTROLS

*For the content of the numbered topics and concepts above, refer to Exhibit 4-4.*
### INFORMATION TECHNOLOGY SECURITY TRAINING MATRIX — Cell 3.4A

| Training Area: **System Life Cycle Security — Implementation**  
| Functional Specialty: **Manage** |
| **Definition** — The system life cycle is a model for building and operating an IT system from its initial inception to its termination and disposal of assets. The model includes six phases: Initiation, Development, Test and Evaluation, Implementation, Operations, and Termination. Life cycle security is the ensemble of processes and procedures which ensures data confidentiality, as needed, as well as data and system integrity, and availability.  
| The implementation phase is the installation of the system into the operational environment in a manner that does not compromise the integrity and effectiveness of the successfully tested security safeguards.  
| **Behavioral Outcome** — Individuals with management responsibilities are able to oversee the implementation and deployment of an IT system in a manner that does not compromise in-place and tested security safeguards.  
| **Knowledge Levels** —  
| 1. Beginning/Intermediate/Advanced — Understand, Ensure, Decide  
| **Sample Learning Objectives** —  
| At the conclusion of this module, individuals will be able to:  
| 1. Beginning/Intermediate/Advanced — Decide whether to continue system deployment if unanticipated circumstances are encountered that compromise security safeguards. Ensure that final implementation in the production environment does not compromise security safeguards.  
| **Sample Job Functions** —  
| • Information Resources Management (IRM) Official, Senior  
| • Information Resources Manager  
| • IT Security Officer/Manager  
| • Program Manager  
<p>| • System Owner |</p>
<table>
<thead>
<tr>
<th>Training Area:</th>
<th>System Life Cycle Security — Implementation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Functional Specialty:</td>
<td>Manage</td>
</tr>
</tbody>
</table>

**IT SECURITY BODY OF KNOWLEDGE TOPICS AND CONCEPTS**

- 3 — SYSTEM ENVIRONMENT
- 4 — SYSTEM INTERCONNECTION
- 5 — INFORMATION SHARING
- 8 — MANAGEMENT CONTROLS
- 9 — ACQUISITION/DEVELOPMENT/INSTALLATION/IMPLEMENTATION CONTROLS
- 10 — OPERATIONAL CONTROLS
- 12 — TECHNICAL CONTROLS

*For the content of the numbered topics and concepts above, refer to Exhibit 4-4.*
<table>
<thead>
<tr>
<th>INFORMATION TECHNOLOGY SECURITY TRAINING MATRIX — <strong>Cell 3.4B</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Training Area:</strong> System Life Cycle Security — Implementation</td>
</tr>
<tr>
<td><strong>Functional Specialty:</strong> Acquire</td>
</tr>
</tbody>
</table>

**Definition** — The system life cycle is a model for building and operating an IT system from its initial inception to its termination and disposal of assets. The model includes six phases: Initiation, Development, Test and Evaluation, Implementation, Operations, and Termination. Life cycle security is the ensemble of processes and procedures which ensures data confidentiality, as needed, as well as data and system integrity, and availability.

The implementation phase is the installation of the system into the operational environment in a manner that does not compromise the integrity and effectiveness of the successfully tested security safeguards.

**Behavioral Outcome** — Individuals with acquisition responsibilities are able to ensure that the system, as implemented, meets all contractual requirements related to the security and privacy of IT resources.

**Knowledge Levels** —
1. Beginning/Intermediate — Know, Review, Decide
2. Advanced — Determine, Interpret, Authorize

**Sample Learning Objectives** —
At the conclusion of this module, individuals will be able to:


2. Advanced — Take action as needed to ensure that accepted products meet contract requirements.

**Sample Job Functions** —
- Contracting Officer
- Contracting Officer’s Technical Representative (COTR)
- IT Security Officer/Manager
- Program Manager
- System Owner
<table>
<thead>
<tr>
<th>INFORMATION TECHNOLOGY SECURITY TRAINING MATRIX — <strong>Cell 3.4B</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Training Area:</strong> System Life Cycle Security — Implementation</td>
</tr>
<tr>
<td><strong>Functional Specialty:</strong> Acquire</td>
</tr>
</tbody>
</table>

**IT SECURITY BODY OF KNOWLEDGE TOPICS AND CONCEPTS**

- 9 — ACQUISITION/DEVELOPMENT/INSTALLATION/IMPLEMENTATION CONTROLS
- 10 — OPERATIONAL CONTROLS
- 12 — TECHNICAL CONTROLS

*For the content of the numbered topics and concepts above, refer to Exhibit 4-4.*
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Definition</strong> — The system life cycle is a model for building and operating an IT system from its initial inception to its termination and disposal of assets. The model includes six phases: Initiation, Development, Test and Evaluation, Implementation, Operations, and Termination. Life cycle security is the ensemble of processes and procedures which ensures data confidentiality, as needed, as well as data and system integrity, and availability. The implementation phase is the installation of the system into the operational environment in a manner that does not compromise the integrity and effectiveness of the successfully tested security safeguards.</td>
<td></td>
</tr>
<tr>
<td><strong>Behavioral Outcome</strong> — Individuals responsible for system design and/or modification are able to participate in the development of procedures which ensure that safeguards are not compromised as they are incorporated into the production environment.</td>
<td></td>
</tr>
<tr>
<td><strong>Knowledge Levels</strong> —</td>
<td></td>
</tr>
<tr>
<td>1. Beginning — Know, Understand, Identify</td>
<td></td>
</tr>
<tr>
<td>2. Intermediate — Interpret, Assess, Apply</td>
<td></td>
</tr>
<tr>
<td>3. Advanced — Determine, Recommend, Select</td>
<td></td>
</tr>
<tr>
<td><strong>Sample Learning Objectives</strong> —</td>
<td></td>
</tr>
<tr>
<td>At the conclusion of this module, individuals will be able to:</td>
<td></td>
</tr>
<tr>
<td>1. Beginning — Identify IT security impacts associated with system implementation procedures.</td>
<td></td>
</tr>
<tr>
<td>2. Intermediate — Participate in the design, development, and modification of safeguards to correct vulnerabilities identified during system implementation.</td>
<td></td>
</tr>
<tr>
<td>3. Advanced — Lead the design, development, and modification of safeguards to correct vulnerabilities identified during system implementation.</td>
<td></td>
</tr>
<tr>
<td><strong>Sample Job Functions</strong> —</td>
<td></td>
</tr>
<tr>
<td>• Database Administrator</td>
<td></td>
</tr>
<tr>
<td>• IT Security Officer/Manager</td>
<td></td>
</tr>
<tr>
<td>• Network Administrator</td>
<td></td>
</tr>
<tr>
<td>• Program Manager</td>
<td></td>
</tr>
<tr>
<td>• Programmer/Systems Analyst</td>
<td></td>
</tr>
<tr>
<td>• System Administrator</td>
<td></td>
</tr>
<tr>
<td>• System Designer/Developer</td>
<td></td>
</tr>
<tr>
<td>• Systems Operations Personnel</td>
<td></td>
</tr>
</tbody>
</table>
## INFORMATION TECHNOLOGY SECURITY TRAINING MATRIX — **Cell 3.4C**

<table>
<thead>
<tr>
<th>Training Area:</th>
<th><strong>System Life Cycle Security — Implementation</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Functional Specialty:</td>
<td><strong>Design &amp; Develop</strong></td>
</tr>
</tbody>
</table>

### IT SECURITY BODY OF KNOWLEDGE TOPICS AND CONCEPTS

- **3**  —  SYSTEM ENVIRONMENT
- **4**  —  SYSTEM INTERCONNECTION
- **5**  —  INFORMATION SHARING
- **8**  —  MANAGEMENT CONTROLS
- **9**  —  ACQUISITION/DEVELOPMENT/INSTALLATION/IMPLEMENTATION CONTROLS
- **10**  —  OPERATIONAL CONTROLS
- **12**  —  TECHNICAL CONTROLS

*For the content of the numbered topics and concepts above, refer to *Exhibit 4-4*.**
### INFORMATION TECHNOLOGY SECURITY TRAINING MATRIX — Cell 3.4D

**Training Area:** System Life Cycle Security — Implementation  
**Functional Specialty:** Implement & Operate

| **Definition** | The system life cycle is a model for building and operating an IT system from its initial inception to its termination and disposal of assets. The model includes six phases: Initiation, Development, Test and Evaluation, Implementation, Operations, and Termination. Life cycle security is the ensemble of processes and procedures which ensures data confidentiality, as needed, as well as data and system integrity, and availability.  
The implementation phase is the installation of the system into the operational environment in a manner that does not compromise the integrity and effectiveness of the successfully tested security safeguards. |

| **Behavioral Outcome** | Individuals responsible for system implementation or operation ensure that approved safeguards are in place and effective as the system moves into production. |

| **Knowledge Levels** |  
| 1. Beginning — Know, Apply, Recognize  
| 2. Intermediate — Identify, Interpret, Decide  
| 3. Advanced — Analyze, Determine, Approve |

| **Sample Learning Objectives** | At the conclusion of this module, individuals will be able to:  
| 1. Beginning — Participate in the implementation of safeguards for an IT system in accordance with the established implementation plan.  
| 2. Intermediate — Identify vulnerabilities resulting from a departure from the implementation plan or that were not apparent during testing. Determine necessary actions to return the implementation process to the established plan or to forward identified vulnerabilities for resolution.  
| 3. Advanced — Examine unresolved system vulnerabilities and determine what corrective action or additional safeguards are necessary to mitigate them. |

| **Sample Job Functions** |  
| Database Administrator  
| IT Security Officer/Manager  
| Network Administrator  
| System Administrator  
| Systems Operations Personnel  
| Technical Support Personnel |
INFORMATION TECHNOLOGY SECURITY TRAINING MATRIX — Cell 3.4D

Training Area: System Life Cycle Security — Implementation
Functional Specialty: Implement & Operate

<table>
<thead>
<tr>
<th>IT SECURITY BODY OF KNOWLEDGE TOPICS AND CONCEPTS</th>
</tr>
</thead>
<tbody>
<tr>
<td>• 3  —  SYSTEM ENVIRONMENT</td>
</tr>
<tr>
<td>• 4  —  SYSTEM INTERCONNECTION</td>
</tr>
<tr>
<td>• 5  —  INFORMATION SHARING</td>
</tr>
<tr>
<td>• 9  —  ACQUISITION/DEVELOPMENT/INSTALLATION/</td>
</tr>
<tr>
<td>IMPLEMENTATION CONTROLS</td>
</tr>
<tr>
<td>• 10 —  OPERATIONAL CONTROLS</td>
</tr>
<tr>
<td>• 12 —  TECHNICAL CONTROLS</td>
</tr>
</tbody>
</table>

For the content of the numbered topics and concepts above, refer to Exhibit 4-4.
### INFORMATION TECHNOLOGY SECURITY TRAINING MATRIX — **Cell 3.4E**

<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Definition</strong> — The system life cycle is a model for building and operating an IT system from its initial inception to its termination and disposal of assets. The model includes six phases: Initiation, Development, Test and Evaluation, Implementation, Operations, and Termination. Life cycle security is the ensemble of processes and procedures which ensures data confidentiality, as needed, as well as data and system integrity, and availability. The implementation phase is the installation of the system into the operational environment in a manner that does not compromise the integrity and effectiveness of the successfully tested security safeguards.</td>
<td></td>
</tr>
<tr>
<td><strong>Behavioral Outcome</strong> — Individuals responsible for review and evaluation are able to analyze system and test documentation to determine whether the system provides adequate and appropriate IT security to support certification and accreditation.</td>
<td></td>
</tr>
<tr>
<td><strong>Knowledge Levels</strong> —</td>
<td></td>
</tr>
<tr>
<td>1. Beginning/Intermediate — Understand, Review, Evaluate</td>
<td></td>
</tr>
<tr>
<td>2. Advanced — Analyze, Decide, Recommend</td>
<td></td>
</tr>
<tr>
<td><strong>Sample Learning Objectives</strong> —</td>
<td></td>
</tr>
<tr>
<td>At the conclusion of this module, individuals will be able to:</td>
<td></td>
</tr>
<tr>
<td>1. Beginning/Intermediate — Review and evaluate the effectiveness of safeguards, the maintainability of IT security features, the adequacy of system documentation, and the efficiency of system security administration.</td>
<td></td>
</tr>
<tr>
<td>2. Advanced — Recommend IT system certification/accreditation and/or measures required to achieve/maintain approval to operate.</td>
<td></td>
</tr>
<tr>
<td><strong>Sample Job Functions</strong> —</td>
<td></td>
</tr>
<tr>
<td>- Auditor, External</td>
<td></td>
</tr>
<tr>
<td>- Auditor, Internal</td>
<td></td>
</tr>
<tr>
<td>- Certification Reviewer</td>
<td></td>
</tr>
<tr>
<td>- Chief Information Officer</td>
<td></td>
</tr>
<tr>
<td>- Designated Approving Authority (DAA)</td>
<td></td>
</tr>
<tr>
<td>- IT Security Officer/Manager</td>
<td></td>
</tr>
<tr>
<td>- Program Manager</td>
<td></td>
</tr>
<tr>
<td>- System Owner</td>
<td></td>
</tr>
</tbody>
</table>
**INFORMATION TECHNOLOGY SECURITY TRAINING MATRIX — Cell 3.4E**

<table>
<thead>
<tr>
<th>Training Area: System Life Cycle Security — Implementation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Functional Specialty: Review &amp; Evaluate</td>
</tr>
</tbody>
</table>

**IT SECURITY BODY OF KNOWLEDGE TOPICS AND CONCEPTS**

- **3** — SYSTEM ENVIRONMENT
- **4** — SYSTEM INTERCONNECTION
- **6** — SENSITIVITY
- **8** — MANAGEMENT CONTROLS
- **9** — ACQUISITION/DEVELOPMENT/INSTALLATION/IMPLEMENTATION CONTROLS
- **10** — OPERATIONAL CONTROLS
- **12** — TECHNICAL CONTROLS

*For the content of the numbered topics and concepts above, refer to Exhibit 4-4.*
### INFORMATION TECHNOLOGY SECURITY TRAINING MATRIX — Cell 3.4F

| Training Area: **System Life Cycle Security — Implementation**  
<table>
<thead>
<tr>
<th>Functional Specialty: <strong>Use</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Definition</strong> — The system life cycle is a model for building and operating an IT system from its initial inception to its termination and disposal of assets. The model includes six phases: Initiation, Development, Test and Evaluation, Implementation, Operations, and Termination. Life cycle security is the ensemble of processes and procedures which ensures data confidentiality, as needed, as well as data and system integrity, and availability.</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>The implementation phase is the installation of the system into the operational environment in a manner that does not compromise the integrity and effectiveness of the successfully tested security safeguards.</td>
</tr>
<tr>
<td><strong>Behavioral Outcome</strong> — Users are able to identify and report security and efficiency concerns encountered during normal operations.</td>
</tr>
</tbody>
</table>
| **Knowledge Levels** —  
| 1. Beginning/Intermediate/Advanced — Know, Apply, Identify |
| **Sample Learning Objectives** —  
| At the conclusion of this module, individuals will be able to:  
| 1. Beginning/Intermediate/Advanced — Follow procedures for using the IT system in a secure manner; identify and report potential security events and efficiency concerns. |
| **Sample Job Functions** —  
| • IT Security Officer/Manager  
<p>| • User |</p>
<table>
<thead>
<tr>
<th>Training Area: System Life Cycle Security — Implementation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Functional Specialty: Use</td>
</tr>
</tbody>
</table>

**IT SECURITY BODY OF KNOWLEDGE TOPICS AND CONCEPTS**

- 6 — SENSITIVITY
- 8 — MANAGEMENT CONTROLS

*For the content of the numbered topics and concepts above, refer to Exhibit 4-4.*
### INFORMATION TECHNOLOGY SECURITY TRAINING MATRIX — Cell 3.5A

|--------------------------------------------------------|-------------------------------|

#### Definition —
The system life cycle is a model for building and operating an IT system from its initial inception to its termination and disposal of assets. The model includes six phases: Initiation, Development, Test and Evaluation, Implementation, Operations, and Termination. Life cycle security is the ensemble of processes and procedures which ensures data confidentiality, as needed, as well as data and system integrity, and availability.

The operations phase includes the ongoing day-to-day use (production) and maintenance or enhancement of the system without compromising the integrity and effectiveness of the installed safeguards.

#### Behavioral Outcome —
Individuals with management responsibilities are able to monitor operations to ensure that safeguards are effective and have the intended effect of balancing efficiency with minimized risk.

#### Knowledge Levels —
1. Beginning — Know, Understand, Decide
2. Intermediate — Direct, Provide, Identify
3. Advanced — Monitor, Evaluate, Select

#### Sample Learning Objectives —
At the conclusion of this module, individuals will be able to:

1. Beginning — Understand the in-place IT security procedures and safeguards and the assignment of responsibilities to ensure that operations personnel are complying with them.

2. Intermediate — Provide leadership and direction to operations personnel by ensuring that IT security awareness, basics and literacy, and training are provided to operations personnel commensurate with their responsibilities.

3. Advanced — Monitor and evaluate the effectiveness of IT security procedures and safeguards to ensure they provide the intended level of protection. Take action as necessary should the level of protection fall below the established minimum.

#### Sample Job Functions —
- Data Center Manager
- IT Security Officer/Manager
- Network Administrator
- Program Manager
- System Administrator
- System Owner
## INFORMATION TECHNOLOGY SECURITY TRAINING MATRIX — Cell 3.5A

|--------------------------------------------------------|------------------------------|

**IT SECURITY BODY OF KNOWLEDGE TOPICS AND CONCEPTS**

- 4 — SYSTEM INTERCONNECTION
- 5 — INFORMATION SHARING
- 8 — MANAGEMENT CONTROLS
- 9 — ACQUISITION/DEVELOPMENT/INSTALLATION/IMPLEMENTATION CONTROLS
- 10 — OPERATIONAL CONTROLS
- 11 — AWARENESS, TRAINING, AND EDUCATION CONTROLS
- 12 — TECHNICAL CONTROLS

*For the content of the numbered topics and concepts above, refer to Exhibit 4-4.*
### INFORMATION TECHNOLOGY SECURITY TRAINING MATRIX — Cell 3.5B

**Training Area:** System Life Cycle Security — Operations  
**Functional Specialty:** Acquire

**Definition**  
The system life cycle is a model for building and operating an IT system from its initial inception to its termination and disposal of assets. The model includes six phases: Initiation, Development, Test and Evaluation, Implementation, Operations, and Termination. Life cycle security is the ensemble of processes and procedures which ensures data confidentiality, as needed, as well as data and system integrity, and availability.

The operations phase includes the ongoing day-to-day use (production) and maintenance or enhancement of the system without compromising the integrity and effectiveness of the installed safeguards.

**Behavioral Outcome**  
Individuals with acquisition responsibilities are able to understand the IT security concerns associated with system operations and to identify and use the appropriate contract vehicle to meet current needs in a timely manner.

**Knowledge Levels**

1. Beginning/Intermediate — Know, Review, Decide  
2. Advanced — Determine, Interpret, Authorize

**Sample Learning Objectives**

At the conclusion of this module, individuals will be able to:


2. Advanced — Take action as needed to ensure that accepted products/services meet contract requirements.

**Sample Job Functions**

- Contracting Officer  
- Contracting Officer’s Technical Representative (COTR)  
- IT Security Officer/Manager  
- Program Manager  
- System Owner
### INFORMATION TECHNOLOGY SECURITY TRAINING MATRIX — **Cell 3.5B**

**Training Area:** System Life Cycle Security — Operations  
**Functional Specialty:** Acquire

#### IT SECURITY BODY OF KNOWLEDGE TOPICS AND CONCEPTS

- **8** — MANAGEMENT CONTROLS
- **9** — ACQUISITION/DEVELOPMENT/INSTALLATION/IMPLEMENTATION CONTROLS
- **10** — OPERATIONAL CONTROLS
- **12** — TECHNICAL CONTROLS

*For the content of the numbered topics and concepts above, refer to Exhibit 4-4.*
### INFORMATION TECHNOLOGY SECURITY TRAINING MATRIX — Cell 3.5C

<table>
<thead>
<tr>
<th>Training Area: System Life Cycle Security — Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Functional Specialty: Design &amp; Develop</td>
</tr>
</tbody>
</table>

**Definition** — The system life cycle is a model for building and operating an IT system from its initial inception to its termination and disposal of assets. The model includes six phases: Initiation, Development, Test and Evaluation, Implementation, Operations, and Termination. Life cycle security is the ensemble of processes and procedures which ensures data confidentiality, as needed, as well as data and system integrity, and availability.

The operations phase includes the ongoing day-to-day use (production) and maintenance or enhancement of the system without compromising the integrity and effectiveness of the installed safeguards.

**Behavioral Outcome** — Individuals responsible for system development are able to make procedural and operational changes necessary to maintain the acceptable level of risk.

**Knowledge Levels** —

1. Beginning/Intermediate — Develop, Know, Understand
2. Advanced — Select, Analyze, Decide

**Sample Learning Objectives** —

At the conclusion of this module, individuals will be able to:

1. Beginning/Intermediate — Design/develop new or modified IT security procedures or safeguards to accommodate changes in operations.

2. Advanced — Modify/select IT security procedures/safeguards that enhance the existing level of security and integrity.

**Sample Job Functions** —

- IT Security Officer/Manager
- Network Administrator
- Programmer/Systems Analyst
- System Administrator
- System Designer/Developer
- Systems Operations Personnel
INFORMATION TECHNOLOGY SECURITY TRAINING MATRIX — Cell 3.5C

Training Area: System Life Cycle Security — Operations
Functional Specialty: Design & Develop

IT SECURITY BODY OF KNOWLEDGE TOPICS AND CONCEPTS

- 3 — SYSTEM ENVIRONMENT
- 4 — SYSTEM INTERCONNECTION
- 5 — INFORMATION SHARING
- 7 — RISK MANAGEMENT
- 9 — ACQUISITION/DEVELOPMENT/INSTALLATION/IMPLEMENTATION CONTROLS

For the content of the numbered topics and concepts above, refer to Exhibit 4-4.
**Information Technology Security Training Requirements**

<table>
<thead>
<tr>
<th>INFORMATION TECHNOLOGY SECURITY TRAINING MATRIX — <strong>Cell 3.5D</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Training Area:</strong> System Life Cycle Security — Operations</td>
</tr>
<tr>
<td><strong>Functional Specialty:</strong> Implement &amp; Operate</td>
</tr>
</tbody>
</table>

**Definition** — The system life cycle is a model for building and operating an IT system from its initial inception to its termination and disposal of assets. The model includes six phases: Initiation, Development, Test and Evaluation, Implementation, Operations, and Termination. Life cycle security is the ensemble of processes and procedures which ensures data confidentiality, as needed, as well as data and system integrity, and availability.

The operations phase includes the ongoing day-to-day use (production) and maintenance or enhancement of the system without compromising the integrity and effectiveness of the installed safeguards.

**Behavioral Outcome** — Individuals responsible for system implementation or operation are able to maintain appropriate safeguards continuously within acceptable levels of risk.

**Knowledge Levels** —

1. Beginning — Know, Participate, Monitor
2. Intermediate — Evaluate, Identify, Execute
3. Advanced — Analyze, Interpret, Recommend

**Sample Learning Objectives** —

At the conclusion of this module, individuals will be able to:

1. Beginning — Participate in maintaining safeguards in accordance with standard operating procedures. Monitor system activity to identify potential IT security events.

2. Intermediate — Evaluate potential IT security events, identify actual security incidents, and take appropriate corrective and recovery actions.

3. Advanced — Analyze IT security incidents or patterns of incidents to determine if remedial actions are needed to correct vulnerabilities and maintain the acceptable level of risk.

**Sample Job Functions** —

- Database Administrator
- IT Security Officer/Manager
- Network Administrator
- System Administrator
- System Operations Personnel
- Technical Support Personnel
- Telecommunications Specialist
**INFORMATION TECHNOLOGY SECURITY TRAINING Matrix — Cell 3.5D**

Training Area: **System Life Cycle Security — Operations**  
Functional Specialty: **Implement & Operate**

### IT SECURITY BODY OF KNOWLEDGE TOPICS AND CONCEPTS

- **7** — Risk Management  
- **8** — Management Controls  
- **9** — Acquisition/Development/Installation/Implementation Controls  
- **10** — Operational Controls  
- **11** — Awareness, Training, and Education Controls  
- **12** — Technical Controls

*For the content of the numbered topics and concepts above, refer to Exhibit 4-4.*
INFORMATION TECHNOLOGY SECURITY TRAINING MATRIX — Cell 3.5E

Training Area: **System Life Cycle Security — Operations**

Functional Specialty: **Review & Evaluate**

**Definition** — The system life cycle is a model for building and operating an IT system from its initial inception to its termination and disposal of assets. The model includes six phases: Initiation, Development, Test and Evaluation, Implementation, Operations, and Termination. Life cycle security is the ensemble of processes and procedures which ensures data confidentiality, as needed, as well as data and system integrity, and availability.

The operations phase includes the ongoing day-to-day use (production) and maintenance or enhancement of the system without compromising the integrity and effectiveness of the installed safeguards.

**Behavioral Outcome** — Individuals responsible for review and evaluation are able to examine the operational system to determine the adequacy and effectiveness of safeguards and to ensure that a consistent and appropriate level of security (i.e., one with an acceptable level of risk) is maintained.

**Knowledge Levels** —

1. Beginning — Understand, Participate, Identify
2. Intermediate — Analyze, Determine, Apply
3. Advanced — Decide, Recommend, Interpret

**Sample Learning Objectives** —

At the conclusion of this module, individuals will be able to:

1. Beginning — Participate in the evaluation of an operational system to determine the adequacy and effectiveness of security safeguards and environment, leading to continued approval to operate (recertification and re-accreditation).

2. Intermediate — Determine the adequacy of security environments and the capability of security strategies, architectures, and safeguards to maintain the integrity of those security environments. Prepare recommendations for system approval decisions.

3. Advanced — Recommend IT system recertification/re-accreditation and/or corrective actions required to achieve/maintain certification/accreditation.

**Sample Job Functions** —

- Auditor, External
- Auditor, Internal
- Certification Reviewer
- Designated Approving Authority (DAA)
- IT Security Officer/Manager
### INFORMATION TECHNOLOGY SECURITY TRAINING MATRIX — Cell 3.5E

**Training Area:** System Life Cycle Security — Operations  
**Functional Specialty:** Review & Evaluate

#### IT SECURITY BODY OF KNOWLEDGE TOPICS AND CONCEPTS

- 7 — RISK MANAGEMENT
- 9 — ACQUISITION/DEVELOPMENT/INSTALLATION/IMPLEMENTATION CONTROLS
- 10 — OPERATIONAL CONTROLS
- 11 — AWARENESS, TRAINING, AND EDUCATION CONTROLS
- 12 — TECHNICAL CONTROLS

*For the content of the numbered topics and concepts above, refer to Exhibit 4-4.*
<table>
<thead>
<tr>
<th>Training Area: <strong>System Life Cycle Security — Operations</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Functional Specialty: <strong>Use</strong></td>
</tr>
</tbody>
</table>

**Definition** — The system life cycle is a model for building and operating an IT system from its initial inception to its termination and disposal of assets. The model includes six phases: Initiation, Development, Test and Evaluation, Implementation, Operations, and Termination. Life cycle security is the ensemble of processes and procedures which ensures data confidentiality, as needed, as well as data and system integrity, and availability.

The operations phase includes the ongoing day-to-day use (production) and maintenance or enhancement of the system without compromising the integrity and effectiveness of the installed safeguards.

**Behavioral Outcome** — Users are able to understand the objectives of and comply with the “rules of behavior” for the system.

**Knowledge Levels** —

1. Beginning/Intermediate/Advanced — Know, Identify, Apply

**Sample Learning Objectives** —

At the conclusion of this module, individuals will be able to:

1. Beginning/Intermediate/Advanced — Follow procedures for using the IT system in a secure manner; identify and report potential security events.

**Sample Job Functions** —

- IT Security Officer/Manager
- User
### INFORMATION TECHNOLOGY SECURITY TRAINING MATRIX — Cell 3.5F

<table>
<thead>
<tr>
<th>Training Area:</th>
<th>System Life Cycle Security — Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Functional Specialty:</td>
<td>Use</td>
</tr>
</tbody>
</table>

**IT SECURITY BODY OF KNOWLEDGE TOPICS AND CONCEPTS**

- 8 — MANAGEMENT CONTROLS
- 10 — OPERATIONAL CONTROLS
- 12 — TECHNICAL CONTROLS

*For the content of the numbered topics and concepts above, refer to Exhibit 4-4.*
**INFORMATION TECHNOLOGY SECURITY TRAINING MATRIX — Cell 3.6A**

**Training Area:** System Life Cycle Security — Termination  
**Functional Specialty:** Manage

**Definition** — The system life cycle is a model for building and operating an IT system from its initial inception to its termination and disposal of assets. The model includes six phases: Initiation, Development, Test and Evaluation, Implementation, Operations, and Termination. Life cycle security is the ensemble of processes and procedures which ensures data confidentiality, as needed, as well as data and system integrity, and availability.

The termination phase comprises the series of steps taken to retire a system when it is no longer needed and to securely and properly archive or dispose of its assets.

**Behavioral Outcome** — Individuals with management responsibilities are able to understand the special IT security considerations and measures required during the shutdown of a system, and effectively plan and direct these activities.

**Knowledge Levels** —

1. Beginning — Understand, Apply, Monitor  
2. Intermediate/Advanced — Validate, Decide, Direct, Approve

**Sample Learning Objectives** —

At the conclusion of this module, individuals will be able to:

1. Beginning — Understand and ensure compliance with the IT security considerations and procedures required for termination of the system.

2. Intermediate/Advanced — Ensure that appropriate and adequate plans and procedures are established, validate the termination plan, and accept the residual level of risk.

**Sample Job Functions** —

- Database Administrator  
- Data Center Manager  
- IT Security Officer/Manager  
- Program Manager  
- System Owner
INFORMATION TECHNOLOGY SECURITY TRAINING MATRIX — **Cell 3.6A**

|--------------------------------------------------------|-----------------------------|

**IT SECURITY BODY OF KNOWLEDGE TOPICS AND CONCEPTS**

- 1 — LAWS AND REGULATIONS
- 5 — INFORMATION SHARING
- 6 — SENSITIVITY
- 7 — RISK MANAGEMENT

*For the content of the numbered topics and concepts above, refer to Exhibit 4-4.*
## INFORMATION TECHNOLOGY SECURITY TRAINING MATRIX — Cell 3.6D

### Training Area: System Life Cycle Security — Termination

#### Functional Specialty: Implement & Operate

### Definition

The system life cycle is a model for building and operating an IT system from its initial inception to its termination and disposal of assets. The model includes six phases: Initiation, Development, Test and Evaluation, Implementation, Operations, and Termination. Life cycle security is the ensemble of processes and procedures which ensures data confidentiality, as needed, as well as data and system integrity, and availability.

The termination phase comprises the series of steps taken to retire a system when it is no longer needed and to securely and properly archive or dispose of its assets.

### Behavioral Outcome

Individuals responsible for IT system operation are able to develop and implement the system termination plan, including security requirements for archiving/disposing of resources.

### Knowledge Levels

1. Beginning — Understand, Comply, Report
2. Intermediate — Apply, Decide, Conduct
3. Advanced — Analyze, Determine, Develop

### Sample Learning Objectives

At the conclusion of this module, individuals will be able to:

1. Beginning — Comply with termination procedures and report any potential IT security incidents or actual breaches to proper authorities.

2. Intermediate — Ensure that hardware, software, data, and facility resources are archived, sanitized, or disposed of in a manner consistent with the system termination plan.

3. Advanced — Develop the system termination plan to ensure that IT security breaches are avoided during shutdown and long-term protection of archived resources is achieved.

### Sample Job Functions

- Contracting Officer’s Technical Representative
- Data Center Manager
- Database Administrator
- FOIA Official
- IT Security Officer/Manager
- Network Administrator
- Privacy Act Official
- Program Manager
- Programmer/Systems Analyst
- Records Management Official
- System Administrator
- Systems Operations Personnel
- Technical Support Personnel
INFORMATION TECHNOLOGY SECURITY TRAINING MATRIX — Cell 3.6D

Training Area: System Life Cycle Security — Termination
Functional Specialty: Implement & Operate

IT SECURITY BODY OF KNOWLEDGE TOPICS AND CONCEPTS

- 5 — INFORMATION SHARING
- 6 — SENSITIVITY
- 7 — RISK MANAGEMENT

For the content of the numbered topics and concepts above, refer to Exhibit 4-4.
**INFORMATION TECHNOLOGY SECURITY TRAINING MATRIX — Cell 3.6E**

| Training Area: **System Life Cycle Security — Termination** |
| Functional Specialty: **Review & Evaluate** |

**Definition** — The system life cycle is a model for building and operating an IT system from its initial inception to its termination and disposal of assets. The model includes six phases: Initiation, Development, Test and Evaluation, Implementation, Operations, and Termination. Life cycle security is the ensemble of processes and procedures which ensures data confidentiality, as needed, as well as data and system integrity, and availability.

The termination phase comprises the series of steps taken to retire a system when it is no longer needed and to securely and properly archive or dispose of its assets.

**Behavioral Outcome** — Individuals responsible for review and evaluation are able to verify the appropriateness of the termination plan and processes used to terminate the IT system securely.

**Knowledge Levels** —

1. Beginning/Intermediate/Advanced — Evaluate, Determine, Verify

**Sample Learning Objectives** —

At the conclusion of this module, individuals will be able to:

1. Beginning/Intermediate/Advanced — Evaluate the termination plan and procedures to ensure that IT security and archival concerns have been appropriately addressed.

**Sample Job Functions** —

- Auditor, External
- Auditor, Internal
- Information Resources Manager
- IT Security Officer/Manager
- Records Management Official
INFORMATION TECHNOLOGY SECURITY TRAINING MATRIX — **Cell 3.6E**

**Training Area:** System Life Cycle Security — Termination  
**Functional Specialty:** Review & Evaluate

---

**IT SECURITY BODY OF KNOWLEDGE TOPICS AND CONCEPTS**

- 1 — LAWS AND REGULATIONS
- 5 — INFORMATION SHARING
- 6 — SENSITIVITY
- 7 — RISK MANAGEMENT

*For the content of the numbered topics and concepts above, refer to Exhibit 4-4.*
CHAPTER 5. EVALUATING TRAINING EFFECTIVENESS

Evaluate: “To determine or fix the value of; to examine carefully”\(^3\)

5.1 Value of Evaluation in a Training Program

Evaluating training effectiveness is a vital step to ensure that the training delivered is meaningful. Training is “meaningful” only when it meets the needs of both the student (employee) and the organization. If training content is incorrect, outdated, or inappropriate for the audience, the training will not meet student or organizational needs. If the delivery vehicle (e.g., classroom or computer-based training) is inappropriate, either in relation to the simplicity/complexity of the content or to the type of audience—or if there is an inadequate mix of vehicles in an agency’s overall training program—the training will not meet needs. Spending time and resources on training that does not achieve desired effects can reinforce, rather than dispel, the perception of security as an obstacle to productivity. Further, it can require the expenditure of far more resources in data or system recovery after a security incident occurs than would have been spent in prevention activities.

All meaningless training is expensive, even where the direct cost outlay, or cost-per-student, may be low. Because agencies cannot afford to waste limited resources on ineffective training, evaluation of training effectiveness should become an integral component of an agency’s IT security training program. A robust training evaluation effort may be the second most effective vehicle for garnering management support for IT security—the first being the occurrence of a serious security incident.

In broader context, attention to IT security training evaluation is in line with a changing focus in the overall field of information technology regarding how results of systems efforts are measured. The focus is beginning to change from being solely a machine view, i.e., measuring the functionality of the technology (e.g., speed, gigabytes), to encompass a people view, i.e., the functionality of the people who use the technology. Thus, in organizations where it is recognized that system utility is affected—or even determined—by users, it becomes apparent that to achieve its full utility, a percentage of the system budget must be devoted to people needs such as training.\(^4\)


5.2 Purposes of Training Effectiveness Evaluation

Meaningfulness, or effectiveness, requires measurement. Evaluating training effectiveness has four distinct but interrelated purposes—to measure:

- The extent to which conditions were right for learning and the learner’s subjective satisfaction;
- What a given student has learned from a specific course or training event, i.e., learning effectiveness;
- A pattern of student outcomes following a specific course or training event; i.e., teaching effectiveness; and
- The value of the specific class or training event, compared to other options in the context of an agency’s overall IT security training program; i.e., program effectiveness.

An evaluation process should produce four types of measurement, each related to one of evaluation’s four purposes, as appropriate for three types of users of evaluation data:

- First, evaluation should yield information to assist the employees themselves in assessing their subsequent on-the-job performance.
- Second, evaluation should yield information to assist the employees’ supervisors in assessing individual students’ subsequent on-the-job performance.
- Third, it should produce trend data to assist trainers in improving both learning and teaching.
- Finally, it should produce return-on-investment statistics to enable responsible officials to allocate limited resources in a thoughtful, strategic manner among the spectrum of IT security awareness, security literacy, training, and education options for optimal results among the workforce as a whole.

5.3 Development of an Evaluation Plan

It is difficult to get “good” information for each of evaluation’s four purposes (above). It is impossible to do so without planning for evaluation. To evaluate student learning, it is first necessary to have written learning objectives, stated in an observable, measurable way as behavioral outcomes: in short, “behavioral objectives.” To evaluate teaching, it is necessary to plan for the collection of trend data, evaluation, and extrapolation. To evaluate return on investment, mission-related goals must be explicitly identified to which the learning objectives
are related. Thus, to obtain “good” information in each of these areas, the process of course development should include the development of an evaluation plan. The remainder of this section provides guidance in the development of an evaluation plan.

### 5.3.1 Behavioral Objectives

The major components of behavioral objectives are: Conditions of Activity, Activity to be Performed, and Level of Success. There are several “schools” of behavioral objectives among educational theorists; however, most agree with the three components, described below.

- **Conditions of Activity**

  This is a written description of existing conditions prior to, and in preparation for, the learning activity. A “snowstorm” metaphor is illustrative. For meteorologists to forecast the arrival of a snowstorm, certain conditions must exist: e.g., relative humidity at a certain level, air temperature, conducive atmospheric conditions. Similarly, certain conditions must be present to forecast training effectiveness. Does the student need a checklist, a set of items to manipulate, or an outline of the information? Does the instructor need audiovisual equipment, handouts, or a classroom with furniture set up in a specific format? Conditions of the learning activity, including computer-based training (CBT), not just “platform” training, must be specific and comprehensive. Keep in mind that if just one of the conditions for a snowstorm is missing, the storm either will not arrive or its force will be diminished. So, too, with learning.

- **Activity to be Performed**

  The evaluation plan must state the activity to be performed in a manner permitting the evaluator to actually observe the behavior that the student is to learn—whether observable in class (teacher as evaluator) or back on the job (supervisor as evaluator). It is difficult, if not impossible, to measure the process of a student changing an attitude or thinking through a task or problem. The evaluator, however, can measure a written exercise, a skill demonstration, a verbal or written pronouncement, or any combination of these outwardly demonstrable activities. He/she cannot take the student’s word for the learned skill, or the simple fact that the student was present and exposed to the skill or information being taught. Rather, the evaluator must observe the skill being performed or the information being applied. (With CBT, evaluation measurement can be programmed to occur at the instructional block level, with subsequent blocks adjusted based on student response. With platform training, adjustments can be made in real time by the instructor based on the nature of student questions during the course. Adjustments can also be made between courses in a student’s training sequence.)
Level of Success

Measures of success should be derived from the individual’s normal work products rather than from classroom testing. This directly ties the individual’s performance to its impact on the organization’s mission. Written behavioral objectives for a learning activity must include a stated level of success. For quantitative skills, must the learner perform successfully every time, or 10 out of 100 times, or 5 out of 10 times in terms of performance requirements or consequences? Risk management requirements should be used to establish the criticality of quantitative skills. For qualitative skills, what distinguishes satisfactory performance from failure, or outstanding performance from satisfactory? Measurements of qualitative skills might include the amount of re-work required, customer satisfaction, or peer recognition of the employee as a source of IT security information.

The nature and purpose of the training activity, and whether it is at a beginning, intermediate, or advanced level, will influence the setting of success measures—a subjective goal. If success levels are not documented, an individual student’s achievement of the behavioral objectives of the learning activity can not be evaluated, nor can the learning activity itself be evaluated within an organization’s overall training program.

In addition to the written objectives suggested above, the evaluation plan should show how the data to be collected are to be used to support the cost and effort of the data collection. This can be related to levels of evaluation, presented below.

5.3.2 Levels of Evaluation

Four levels of evaluation, in order of complexity, are:

- Level 1: End-of-Course Evaluations (Student Satisfaction)
- Level 2: Behavior Objective Testing (Learning Effectiveness, which is also a measure of Teaching Effectiveness)
- Level 3: Job Transfer Skills (Performance Effectiveness)
- Level 4: Organizational Benefit (Training Program Effectiveness)

Altogether, the four levels match the four purposes of training evaluation (described in Section 5.2) in a staged manner. These levels are as follows.
Level 1: End-of-Course Evaluations (Student Satisfaction)

A common term for this type of evaluation is “the ‘Smiley Face’ evaluation.” Likert Scale-type forms ask the student to check a range of options from “poor” to “excellent” (or vice versa) to indicate how he/she felt about the class, the computer-based courseware, or whatever the learning activity was. The response data is an indicator of how the learning activity is received by the student. The responses also reveal if the conditions for learning were correct. Some of the questions in this level of evaluation ask about the student’s satisfaction with the training facility and instructor (if classroom training), the manner of presentation of the content, and whether or not course objectives were met in relation to the student’s expectations. Although this type of evaluation does not provide in-depth data, it does provide rapid feedback from the learner’s perspective.

Measurement of training effectiveness depends on an understanding of the background and skill level of the training audience. For example, technical training provided to an audience of systems analysts and programmers will have a different level of effect than that provided to an audience of accountants. Basic demographic data may be collected at either course commencement or conclusion, but information regarding the learners’ satisfaction with the course and course material should be collected at the end of the course.

Level 2: Behavior Objective Testing (Learning and Teaching Effectiveness)

This level of evaluation measures how much information or skill was transmitted from the training activity to the learner. The evaluation should be in various formats relative to the level of training. In an IT Security Basics and Literacy course, for example, participants could be given a pre-test and a post-test of multiple choice items or fill-in-the-blank statements. At an intermediate or advanced training level, participants should be given some sort of performance test, such as a case study to solve. At the education level, essay questions exploring concepts would be appropriate. The evaluation format must relate back to the behavioral objectives of the learning activity which, in turn, drive the content being presented. The Level 2 evaluation also provides instant feedback, but it is more objective than a Level 1 evaluation: it assesses how much the student remembered or demonstrated by skill performance by the end of the program—not how he/she felt about it. As previously noted, Level 2 evaluation can be built into each block of instruction and does not need to wait until the end of a course.

A Level 2 evaluation measures success in transference of information and skills to the student. It enables the evaluator to determine if a given student may need to repeat the course, or perhaps attend a different type of learning activity presenting the same material in a different format. The evaluator should be able to see if a pattern of transference problems emerges, and determine whether or not the course itself may need to be reconfigured or perhaps dropped from an organization’s training program.
Behavior objective testing is possibly the most difficult measurement area to address. It is relatively easy to test the knowledge level of the attendees after completing a course or block of instruction but it is not easy to determine when that learning took place. An attendee may have had knowledge of the subject area before receiving the instruction so that the course had little or no impact. Thus, information collected solely at the conclusion of a course/instructional block must be examined relative to the attendee’s background and education.

To better determine the learning impact of a specific course or instructional block, an approach is to use pre/post testing in which testing is performed at the outset, and the results are compared to testing conducted at the conclusion of instruction.

Testing of an attendee’s knowledge of a particular subject area by including questions or tasks where there is a single right answer or approach is appropriate for almost all testing situations, especially at the beginning and intermediate levels. Questions regarding selection of the “best” answer among possible options should be reserved for those training environments where there is opportunity for analysis regarding why a particular answer is better than other answers.

**Level 3: Job Transfer Skills** (Student Performance Effectiveness)

This evaluation is the first level which asks for more than student input. At this level, the evaluator, through a structured questionnaire usually administered 30 to 60 days following the training activity, asks the supervisor about the performance of the employee(s) relative to the behavioral objectives of the course. This is a “before” and “after” job skills comparison. In some cases this information is difficult to obtain, especially when employees’ job functions and grade levels permit them considerable autonomy, without direct supervision. When supervisors observe only the final output of employee actions, developing a valid questionnaire can present a particular challenge. When accomplished successfully, a Level 3 evaluation should begin to show the extent to which the learning activity benefits the organization as well as the employee.

Questions appropriate for the learner’s supervisor might include:

- Has the learner used the knowledge obtained in the course to accomplish job tasks?

- Has the learner’s performance improved since taking the course?

**Level 4: Organizational Benefit** (Training Program Effectiveness)

Level 4 evaluations can be difficult to undertake and hard to quantify. They can involve structured, follow-up interviews with students, their supervisors, and colleagues. They can
Involve comparison by a subject-matter expert of outputs produced by a student both before and after training. They can involve some form of benchmarking, or evaluation of the particular training activity in relation to other options for a particular job performance measure. In all cases they involve quantifying the value of resulting improvement in relation to the cost of training. Level 4 evaluations, properly designed, can help senior management officials to answer such hypothetical questions as: “Is it more cost-effective to devote limited training resources to the education of a single, newly-appointed IT security specialist in this organization, or to devote the same resources to security basics and literacy training of all employees in the organization?”; or “Is it a better return on investment to train ‘front-end’ systems designers and developers in building security rules commensurate with the sensitivity of the system, or to train ‘back-end’ users in compliance with currently existing system rules?”

Determination of the purpose and objectives of a Level 4 evaluation, as well as the number of variables and the method of measurement of skill level, should only be done following completion of Level 3 evaluation(s), utilizing the findings thereof.

5.4 Implementation of Evaluation Planning

The information in Exhibit 5-1 should help in starting a comprehensive evaluation effort of an organization’s IT security training program. Each cell suggests the overall skill objective which should be attained by the cell evaluator (e.g., instructor, or the student’s supervisor, as appropriate) and/or the overall program evaluator with respect to the various types of learning programs. Each cell also produces a variety of specific information and requires different tools.

Because of the vast amount of data collected, evaluation tools usually consist of a series of questions which require response on a Likert-type scale. This scale, from one to five (one being very good; five being not good, or vice versa), allows the evaluator to prioritize the usefulness of the overall training program and the specific courses or learning events or components within it. Each tool is program- and site-specific.

A practical method to use is to choose a starting point in Exhibit 5-1, beginning with a type of training the organization currently offers; then find an evaluation tool appropriate to a cell at that level and borrow or adapt the concepts presented from already-developed tools. Samples of some of these evaluation tools appear as Exhibits 5-2 and 5-3. Agency training staff may be able to help locate other tools.

(Text continues after exhibits, on page 170.)
<table>
<thead>
<tr>
<th>Levels of Evaluation</th>
<th>Type of Training</th>
<th>Exhibit 5-1 Evaluation Objectives</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td><strong>Level 1: Student Satisfaction</strong></td>
</tr>
<tr>
<td>Basics/Literacy</td>
<td>How well did the student think he/she grasped the security concepts? For CBT, how many attempts did it take for the student to pass the test?</td>
<td>How did the majority of students perform on the test, e.g., do aggregated post-test answers show sufficient improvement over pre-test answers?</td>
</tr>
<tr>
<td>Training</td>
<td>How well did the training program fit the student’s expectations?</td>
<td>Did the training program demonstrably and sufficiently increase the scope and/or depth of the student’s skill set?</td>
</tr>
<tr>
<td>Education</td>
<td>Did the course of study advance the student’s career development or professional qualifications in IT security?</td>
<td>Could the student apply the increased knowledge to a real-world situation adequately?</td>
</tr>
<tr>
<td>Exhibit 5-2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sample Questionnaire — Level 1 Evaluation</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Training Assessment by Student</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

1. Indicate your highest level of education:
   - High School graduate or less
   - Bachelor’s Degree
   - Some college/technical school
   - Master’s Degree
   - Associate degree or technical certification
   - Doctorate

2. Indicate the total number of courses you have completed in subject areas related to this training:
   - 0
   - 1-4
   - 5-10
   - 11-15
   - More than 15

3. Indicate how long it has been since you took a course in the subject area of this training:
   - This is my first course in this subject
   - Less than 1 year
   - 1-3 years
   - 4-6 years
   - More than 6 years

4. Indicate the extent of your work experience in the general subject areas of this training:
   - None
   - Less than 1 year
   - 1-3 years
   - 4-6 years
   - More than 6 years

5. For my preparation and level of knowledge, the training was:
   - Too elementary
   - Somewhat elementary
   - Somewhat difficult
   - About right
   - Too difficult

6. The pace at which the subject matter was covered was:
   - Too slow
   - Somewhat slow
   - Somewhat fast
   - About right
   - Too fast

7. For what I got out of this training, the workload was:
   - Light
   - About right
   - Heavy

8. Considering my previous experience with this subject matter, the course content was:
   - Out of date
   - Somewhat current
   - State-of-the-art
   - Not applicable (no previous experience)
   - Current

*Continued on next page.*
**Exhibit 5-2  (Continued)**  
**Sample Questionnaire — Level 1 Evaluation**  
**Training Assessment by Student**

9. Which of the following best describes the usefulness of this training for your job:
   - [ ] Not particularly useful
   - [ ] Somewhat useful
   - [ ] Very useful
   - [ ] Essential

10. How much did you learn from this training:
   - [ ] Not much
   - [ ] A moderate amount
   - [ ] A great deal

**Student Perception of Instructor**

<table>
<thead>
<tr>
<th>Extent to which the instructor successfully:</th>
<th>Excellent</th>
<th>Good</th>
<th>Fair</th>
<th>Poor</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Presented material in an organized manner</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2. Communicated knowledge of the subject matter</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3. Made difficult concepts understandable</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4. Used class time effectively</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5. Stimulated interest in the subject area</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6. Demonstrated positive attitude toward participants</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7. Overall, I would rate this instructor</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Student Perception of Course Quality**

<table>
<thead>
<tr>
<th>Course content:</th>
<th>Excellent</th>
<th>Good</th>
<th>Fair</th>
<th>Poor</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Clarity of course objectives</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2. Agreement between course objectives and course content</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3. Agreement between Tests/Exams and course objectives</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4. Degree to which the organization of the course enhanced my</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5. Opportunities to practice/apply course content during</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6. Effectiveness of textbook(s), handouts, or other material</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7. Quality of classroom/lab facilities</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8. Overall, I would rate this course</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Exhibit 5-3
Sample Questionnaire — Level 3 Evaluation
Training Assessment by Supervisor

**SECTION I - COURSE RELATION TO JOB REQUIREMENTS**

1. What was the chief reason for nominating the employee for this course?
   - Information is required in present job
   - Information is required in new job
   - Course provides prerequisite or background for other training
   - Course is required to meet certification
   - Course provides general career development
   - Other (please specify) ________________________________

2. Considering past experience/training and present/future job assignments, how well timed was this course in the employee’s career?
   - Took before needed
   - Took when needed
   - Needed course earlier, but wasn’t offered
   - Needed course earlier, but couldn’t get in
   - Didn’t need course and probably will never use it
   - Unable to assess at this time

3. Which of the following best describes the usefulness of this training for the employee’s job?
   - Essential
   - Very useful
   - Somewhat useful
   - Not particularly useful
   - Unable to assess at this time

4. How frequently does the employee need the skills or knowledge acquired in this course?
   - Daily
   - Weekly
   - Periodically
   - Not currently used, but needed for background or future use
   - Criteria does not apply to this course

*Continued on next page.*
SECTION II - COURSE IMPACT ON EMPLOYEE PERFORMANCE

Rate the degree to which the employee’s IT security-related job performance was affected by the training in this course.

<table>
<thead>
<tr>
<th>Job Impact</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Knowledge of IT security-related job duties</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Technical skills (include applicable language-related skills)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Productivity</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Accuracy</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Use of job aids (e.g., reference aids, software applications)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Overall work quality</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Legend:
1 = Greatly improved 3 = Moderately improved 5 = Not applicable
2 = First-time impact 4 = No change

SECTION III - RETURN ON TRAINING INVESTMENT

1. How would you describe the trade-off between the employee’s time away from the job versus IT security-related benefits from taking this course?
   - Great benefits from training offset employee time away from the job
   - Modest benefits from training offset employee time away from the job
   - Benefits from training did not offset employee time away from the job
   - Do not have enough information to respond
   - Benefits from this course can not be measured in this manner

2. How would you respond if another employee from your area needed/wanted to take this course?
   - Would definitely nominate others if I knew the course was applicable to their duties
   - Would not nominate others because _____________________________
   - Would nominate others only if the following course changes were made:
     ____________________________________________________________
     ____________________________________________________________
   - Do not have enough information to decide.

Continued on next page.
### Exhibit 5-3  (Continued)

**Sample Questionnaire — Level 3 Evaluation**

**Training Assessment by Supervisor**

<table>
<thead>
<tr>
<th>3. How knowledgeable were you about the course content before receiving this form?</th>
</tr>
</thead>
<tbody>
<tr>
<td>☐ I had read the catalog description or brochure and knew the expected behavioral outcome.</td>
</tr>
<tr>
<td>☐ I had read the catalog description or brochure but did not know the expected behavioral outcome.</td>
</tr>
<tr>
<td>☐ I knew the overall purpose or goal of the course but did not read a detailed description of it and did not know the expected behavioral outcome.</td>
</tr>
<tr>
<td>☐ I only knew the course existed.</td>
</tr>
<tr>
<td>☐ I knew nothing about the course until I received this form.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>4. As a supervisor, how satisfied are you with the training results from this course?</th>
</tr>
</thead>
<tbody>
<tr>
<td>☐ Highly satisfied</td>
</tr>
<tr>
<td>☐ Satisfied</td>
</tr>
<tr>
<td>☐ Dissatisfied</td>
</tr>
<tr>
<td>☐ Highly dissatisfied</td>
</tr>
<tr>
<td>☐ Unsure</td>
</tr>
</tbody>
</table>
5.5 Summary

Evaluation is undertaken to measure the effectiveness of an agency’s or organization’s IT security training program, i.e., the extent to which the overall program and its respective components are either meaningful or a waste of the organization’s limited training resources. The employee (student) must be asked their view of each learning event (Level 1 and Level 2), the supervisor their view of the event (Level 3), and the organization its view of the event (Level 4) in relation to return on investment. In this process, both quantitative and qualitative data will be collected. At Levels 3 and 4, data collection will be longitudinal. As important as it is for the evaluator to collect the raw data, analysis and application of the collected data is where the IT Security Program Manager and senior officials get the organization’s money’s worth out of its IT security training program. Evaluation planning in advance of the event(s) to be evaluated is essential.

To assist in this regard, Exhibit 5-4 on the following page illustrates and correlates the elements of training effectiveness evaluation that have been discussed in this chapter, i.e., the four purposes of evaluation and four types of data needed for measurement (from section 5.2), the three behavioral objectives (from subsection 5.3.1), and the four levels of evaluation (from subsection 5.3.2) along with the evaluation tools or instruments associated with each level (from section 5.4).

5.6 Chapter References

For further information about training evaluation tools, the following resources are suggested as a point of departure. This is not an exhaustive listing.


### Exhibit 5-4
**Correlation of Evaluation Elements**

<table>
<thead>
<tr>
<th>Purpose — to measure</th>
<th>Data Needed for Measurement</th>
<th>Required to Plan Evaluations</th>
<th>Levels of Evaluation/ Type of Evaluation Tool</th>
</tr>
</thead>
</table>
| **Learner Satisfaction** | • Data to assess conditions for learning and student subjective learning assessment | Written behavioral objectives:  
  • Conditions of activity  
  • Activity to be performed  
  • Level of success | Level 1 - End of Course Evaluations  
  • Likert-scale forms |
| **Learning/Teaching Effectiveness**  
(What a student has learned) | • Data to measure objectively how much knowledge/skill was transmitted to the learner | Written behavioral objectives:  
  • Conditions of activity  
  • Activity to be performed  
  • Level of success | Level 2 - Behavior Objective Testing  
  • Pre-test/post-test  
  • Performance test (e.g., case study)  
  • Essay questions |
| **Job Performance Effectiveness**  
(Pattern of student behavioral outcomes) | • Trend data for trainer improvement | Identified steps for trend data gathering, evaluation, and extrapolation | Level 3 - Job Transfer Skills  
  Supervisor assessment - structured questionnaire for supervisor for “before and after” skills comparison |
| **Program Effectiveness**  
(Value of training event compared to other options) | • Return on investment data for optimal resource allocation | Mission-related goals tied to explicit learning objectives | Level 4 - Organizational Benefit  
  • Structured follow-up interviews with students, supervisors, and colleagues  
  • Comparison of student outputs (before and after training)  
  • Benchmarking |
# Index

ABC’s ............................................................... vii, 27-39
Accreditation ................................................................. 51, 119, 121, 133, 145
Acquire ................................................................. 9, 28, 43, 61, 62, 75, 76, 85, 86, 97, 98, 107, 108, 127, 128, 139, 140
Acquisition/installation/implementation controls ........................................ 36, 37
Adult learning ........................................................................ 9, 20
Audit .................................................................................. 28, 29, 39, 52, 53, 63, 65
Auditor, external ................................................................... 47, 67, 81, 91, 101, 113, 121, 133, 145, 153
Auditor, internal ................................................................... 47, 63, 67, 79, 81, 91, 101, 113, 121, 133, 145, 153
Authorization ........................................................................ 29, 53
Availability ........................................................................ 3, 27-29, 35, 36, 50
Awareness ........................................................................ iii, v, 3, 5, 7, 9, 13-15, 18, 25-27, 30, 36, 37, 43, 52, 68, 74, 78, 80, 82, 84, 90, 92, 102, 137, 138, 144, 146, 158

Behavioral objectives ............................................................... vi, 159-162, 170, 171

Certification ........................................................................ 16, 38, 47, 51, 67, 113, 119, 121, 133, 145, 165, 167
Certification reviewer ................................................................ 47, 67, 113, 119, 121, 133, 145
Chief Information Officer ............................................................... iv, 47, 59, 77, 79, 83, 87, 133
Computer Security Act ................................................................ 3, 30, 43, 59, 69
Confidentiality ........................................................................ 3, 27, 29, 35, 36, 50, 53
Contracting Officer .................................................................. 47, 61, 85, 97, 107, 127, 139
Core set of IT security terms and concepts ................................ 47, 61, 75, 85, 97, 107, 127, 139
COTR ....................................................................................... 8, 9, 26, 32, 33

DAA ................................................................................... 27, 28, 38, 47, 113, 121, 133, 145
Data Center Manager ................................................................... 47, 111, 137, 149, 151
Database Administrator ................................................................. 47, 111, 119, 129, 131, 143, 149, 151
Design and develop ................................................................... 9, 43, 117
Designated Approving Authority .................................................. 47, 113, 119, 121, 133, 145
Development ........................................................................ iv-7, 9, 16, 25, 33, 36, 37, 41, 43, 44, 46, 48, 51, 52, 62-64, 68, 73, 74, 76-80, 82, 84, 86-88, 90, 92, 95-103, 105-123, 125-135, 137-147, 149, 151, 153, 158, 159, 164, 167, 170

Education ................................................................................ iii-6, 9, 13, 14, 16-21, 26, 43, 52, 68, 74, 78, 80, 82, 84, 90, 92, 102, 138, 144, 146, 158, 161-165
Evaluation ................................................................ ............. vi-6, 9, 38, 44, 50, 61, 67, 81, 91, 157-171

Freedom of Information Act Official ............................................... 47, 109

Implement and operate ............................................................... 9, 43
Information Technology Security Training Requirements

**Implementation** ........................................ vi, 9, 31, 36-38, 43, 44, 51, 62-65, 68, 74-76, 78-80, 82-92, 95-103, 105-115, 117-123, 125-147, 149, 151, 153, 163

**Individual accountability** .................................. 27, 29, 34, 37, 39, 51, 69

**Information Resources Management Official, Senior** ........................................ 47

**Information Resources Manager** .................................. 47, 59, 63, 67, 69, 73, 75, 77, 79, 83, 85, 89, 95, 101, 105, 125, 153

**Information sharing** .................................. 34, 49, 62, 64, 68, 74, 76, 78, 82, 84, 90, 92, 96, 98, 100, 102, 106, 110, 112, 120, 122, 126, 130, 132, 138, 142, 150, 152, 154

**Initiation** .................................. 37, 44

**Integrity** .................................. 3, 27, 29, 31, 35, 36, 50, 53

**IT security basics and literacy** .................................. 5, 9, 25, 161

**IT security body of knowledge topics and concepts** .................................. vii, 9, 46, 48-53

**IT Security Officer/Manager** .................................. 47

**IT security program** .................................. 7-9, 17, 26, 29, 34, 43, 48, 60, 64, 73-92, 96, 98, 100, 102, 104, 110, 170

**Job function** .................................. vi-6, 10, 26, 27, 29, 30, 37, 39, 46, 47

**KSAs** .................................. iii, 43, 44

**Laws and regulations** .................................. v, 27, 30, 33, 43, 48, 57, 59, 60, 62-70, 74, 82, 84, 86, 90, 92, 150, 154

**Learning continuum** .................................. v-vii, 9, 11, 13, 16, 17, 19, 25, 43, 44

**Learning styles** .................................. v-vii, 9, 11, 13, 16, 17, 19, 25, 43, 44

**Levels of evaluation** .................................. vi, 6, 160, 170, 171

**Life cycle security** .................................. v, 9, 93, 95-101, 103, 105-154

**Likert Scale** .................................. 161

**Manage** .................................. iii, 27, 31, 43, 51, 59, 60, 73, 74, 83, 84, 95, 96, 105, 106, 125, 126, 137, 138, 149, 150


**Management controls** .................................. 36, 51, 62

**Model** .................................. 1, iii, v, 6, 7, 9, 11, 13, 14, 26, 27, 30, 37, 43, 44

**Network Administrator** .................................. 47, 65, 89, 111, 119, 129, 131, 137, 141, 143, 151

**Operational controls** .................................. 36, 38, 52

**Operations** .................................. 28, 31, 38, 44, 47, 65, 89

**Organization and IT Security** .................................. 33

**Performance-based** .................................. 1, iii, 6, 7, 9
Planning .................................................. vii, 9, 32, 36, 38, 49, 51, 52, 73-82, 101, 158, 163, 170
Privacy Act Official .......................................................... 47, 109, 151
Program Manager .................................................. 16, 17, 47, 63, 73, 83, 89, 95, 99, 113, 125, 127, 129, 133, 137, 139, 149, 151, 170
Programmer/Systems Analyst .......................... 47, 63, 65, 109, 117, 119, 129, 141, 151

Records Management Official .............................. 47, 109, 151, 153
Results-based learning ......................................................... v, 5
Review .................................................. 7, 9, 43, 47, 51, 65, 67-69, 73, 81-83, 85, 91, 92, 101, 102, 105, 109, 113, 114, 121, 122, 127, 133, 134, 139, 145, 146, 153, 154
Review and evaluate .................................................. 9, 43, 113, 133
Risk management .................................................. 4, 27, 31, 35, 50, 60, 62, 66, 68, 74, 78, 80, 82, 84, 88, 90, 92, 102-104, 106, 110, 114, 120, 142, 144, 146, 150, 152, 154, 160
Roles and responsibilities .................................................. 3, 5, 9, 27, 37, 43, 51
Role-based training ....................................................... v, 9, 16, 25, 33, 41, 43
Rules of behavior ......................................................... 34, 37, 51

Security basics ....................................................... v, 5, 9, 16, 23, 25, 26, 43, 46, 161, 163
Security literacy .......................................................... 25, 26, 158
Security responsibility ................................................... 46
Sensitivity .................................................. 3, 15, 35, 50, 51, 62, 64, 68, 74, 78, 82, 84, 90, 92, 96, 98, 100, 102, 104, 106, 110, 116, 134, 136, 150, 152, 154, 163
Separation of duties ......................................................... 27, 29, 37, 39, 51
Source Selection Board Member ........................................ 47, 61, 75, 85, 107
System Administrator .................................................. 47, 65, 89, 111, 119, 129, 131, 137, 141, 143, 151
System Designer/Developer ........................................ 47, 63, 95, 97, 99, 105, 109, 111, 117, 129, 141
System environment ...................................................... 49, 62, 64, 68, 74, 76, 78, 82, 84, 86, 90, 92, 98, 100, 102, 110, 112, 120, 122, 126, 130, 132, 134, 142
System interconnection .................................................. 34, 49, 64, 68, 74, 76, 78, 82, 84, 90, 92, 98, 100, 102, 106, 110, 112, 120, 122, 126, 130, 132, 134, 138, 142
System Owner ....................................................... 47, 69, 73, 89, 95, 97, 99, 101, 103, 105, 107, 113, 121, 123, 125, 127, 133, 137, 139, 149
Systems Operations Personnel ........................................ 47, 65, 129, 131, 141, 151

Technical controls ..................................................... 34, 36, 39, 53
Technical Support Personnel ........................................ 47, 65, 111, 131, 143, 151
Telecommunications Specialist ..................................... 47, 75, 143
Termination .................................................. 38, 44
Test and evaluation ...................................................... 38
Training .................................................. 1, iii, v-vii, 3-10, 13-20, 25-27, 29-33, 36, 37, 41, 43-47, 52, 55, 57, 59-71, 73-93, 95-155, 157-171
Training assessment ..................................................... vii, 165-169
Training effectiveness .................................................... vi, 8, 9, 157-159, 161, 170
Information Technology Security Training Requirements

Training effectiveness evaluation ............................................... vi, 158, 170

**NIST Technical Publications**

**Periodical**

**Journal of Research of the National Institute of Standards and Technology**—Reports NIST research and development in those disciplines of the physical and engineering sciences in which the Institute is active. These include physics, chemistry, engineering, mathematics, and computer sciences. Papers cover a broad range of subjects, with major emphasis on measurement methodology and the basic technology underlying standardization. Also included from time to time are survey articles on topics closely related to the Institute’s technical and scientific programs. Issued six times a year.

**Nonperiodicals**

**Monographs**—Major contributions to the technical literature on various subjects related to the Institute’s scientific and technical activities.

**Handbooks**—Recommended codes of engineering and industrial practice (including safety codes) developed in cooperation with interested industries, professional organizations, and regulatory bodies.

**Special Publications**—Include proceedings of conferences sponsored by NIST, NIST annual reports, and other special publications appropriate to this grouping such as wall charts, pocket cards, and bibliographies.

**National Standard Reference Data Series**—Provides quantitative data on the physical and chemical properties of materials, compiled from the world’s literature and critically evaluated. Developed under a worldwide program coordinated by NIST under the authority of the National Standard Data Act (Public Law 90-396). NOTE: The Journal of Physical and Chemical Reference Data (JPCRD) is published bimonthly for NIST by the American Chemical Society (ACS) and the American Institute of Physics (AIP). Subscriptions, reprints, and supplements are available from ACS, 1155 Sixteenth St., NW, Washington, DC 20056.

**Building Science Series**—Disseminates technical information developed at the Institute on building materials, components, systems, and whole structures. The series presents research results, test methods, and performance criteria related to the structural and environmental functions and the durability and safety characteristics of building elements and systems.

**Technical Notes**—Studies or reports which are complete in themselves but restrictive in their treatment of a subject. Analogous to monographs but not so comprehensive in scope or definitive in treatment of the subject area. Often serve as a vehicle for final reports of work performed at NIST under the sponsorship of other government agencies.

**Voluntary Product Standards**—Developed under procedures published by the Department of Commerce in Part 10, Title 15, of the Code of Federal Regulations. The standards establish nationally recognized requirements for products, and provide all concerned interests with a basis for common understanding of the characteristics of the products. NIST administers this program in support of the efforts of private-sector standardizing organizations.

*Order the following NIST publications—FIPS and NISTIRs—from the National Technical Information Service, Springfield, VA 22161.*


**NIST Interagency or Internal Reports (NISTIR)**—The series includes interim or final reports on work performed by NIST for outside sponsors (both government and nongovernment). In general, initial distribution is handled by the sponsor; public distribution is handled by sales through the National Technical Information Service, Springfield, VA 22161, in hard copy, electronic media, or microfiche form. NISTIR’s may also report results of NIST projects of transitory or limited interest, including those that will be published subsequently in more comprehensive form.
Training Your Employees: Privacy Awareness Tips for Employees

As customer service employees, you are guardians of sensitive customer information and can be our first line of defense against its fraudulent use. Please review the following tips for safeguarding customer information so we can be sure we are giving our customers the utmost protection.

**Log Off.** Don't leave sensitive customer information on your desk or computer screen unattended. Log off the system if you need to leave your desk.

**Shred.** Foil "dumpster divers" by shredding any documents — such as account statements and applications — before discarding them.

**Securely Store.** Keep all documents and reports safe by locking file cabinets.

**Put Away Documents.** When you are finished helping one customer, put away any documents containing that customer's personal information before helping the next customer.

**Authenticate.** Never give customer information over the phone unless you have initiated the call and have followed the appropriate identification procedures.

**Follow Procedures.** Make sure all identification provided is legitimate and meets our institution's criteria.

**Scrutinize.** Carefully scrutinize all requests for account related information or change of address. Emphasize proper identification.

**Resist Intimidation.** Don't be intimidated by requests for information from someone claiming to be with the government or a law enforcement agency. Financial institutions are not required to provide such information without a subpoena.

**Report Suspicious Activity.** Tell your manager of any suspicious change of address requests, such as someone who cannot provide critical identifying information. Chances are good that same person will try again with another bank employee.

Training Your Employees: Spotting and Avoiding Pretext Calls

by Robert Douglas, CEO, American Privacy Consultants

All financial institutions need to be aware of the use of pretext calls by information brokers and identity thieves to gain unauthorized and often illegal access to customer information. The financial services industry takes the threat of unauthorized access to customer information seriously and was a leader in supporting the passage of the provisions within the Gramm-Leach-Bliley Act that make it a crime to obtain or attempt to obtain a customer's information through the use of pretext against a financial institution or against the customer of a financial institution.

All employees of the financial services industry need to:

1. Understand the definition of pretext as it applies to financial institutions;
2. Understand why pretext callers use pretext to access customer information;
3. Understand the types of pretext methods used;
4. Know how to spot possible pretext calls;
5. Know what to do when a possible pretext call is detected; and
6. Be aware of possible ways to stop pretext calls.

**Defining Pretext in the Financial Services Industry**

Pretext is the use of deception to cover the true reason for a given action. Under Title V of the GLB Act, the use of pretext to illegally gain access to customer information maintained by financial institutions is a felony punishable by fine and/or imprisonment. Further, it is a felony to illegally induce the customer of a financial institution to reveal his or her own customer information. All employees of the financial services industry need to understand and be able to define pretext and pretext calls in order to protect customer information.

The most common pretext is a caller falsely informing an employee of a financial institution that the caller is a customer attempting to gain authorized access to his or her own information. The goal is to convince the financial institution employee to provide customer information that the employee would not provide if the employee knew the true identity of the caller. In many cases the pretext caller posing as a legitimate customer will have obtained some biographical and relevant account information from other sources or by means of identity theft in order to perform the pretext and further convince the financial institution that the pretext caller is the legitimate customer.

**PRETEXT EXAMPLE**

Bob Smith is the holder of an account at Main Street Bank. Joe Imposter obtains from various sources Mr. Smith's full name, social security number, address, and date of birth. Joe Imposter, using pretext, calls Main Street Bank and identifies himself as Mr. Smith.

The bank, for security reasons, asks for personal information that the bank mistakenly believes only Mr. Smith could know. Joe Imposter, armed with Mr. Smith's biographical data, is able to convince the bank that he is actually Mr. Smith. The bank then provides Joe Imposter with any information he requests on Mr. Smith's account.

**Pretext Calls are Used to Obtain and Sell Customer Information and for Identity Theft**

Historically, information brokers, private investigators, collection agencies, and identity thieves have most commonly used pretext to obtain customer information from financial institutions.

The largest number of calls appear to be placed by information brokers who have developed a specialty in obtaining information on individuals and businesses and reselling it for a profit. Much of the information accessed and sold by information brokers is legally obtained from publicly available data that have been compiled into proprietary databases. However, prior to the passage of the GLB Act, it was determined that many information brokers were routinely advertising their ability to specifically obtain financial institution customers' information. This information was being sold to anyone willing to pay for it.

Private investigators and collection agencies have also been traditional users of pretext to gain access to customer information. In many cases, attorneys or others seeking to locate the financial assets of an individual or business as part of a financial investigation have retained private investigators or collection agencies. Records obtained as part of investigations of the use of pretext have shown that pretext by private investigators and collection professionals is often used to determine if the customer of a financial institution has assets available to cover a monetary judgment entered by a Court, whether the customer has assets being hidden from a spouse or child, or is engaging in bankruptcy fraud by hiding undeclared assets.

Finally, identity thieves use pretext to obtain customer information as a means of committing financial crimes such as check and credit card fraud. Recent cases have disclosed identity thieves using pretext calls to financial institutions in order to raise credit card limits prior to using the credit cards to make illegal purchases or to illegally obtain cash.
Why Every Employee Should Care

The number of pretext calls to financial institutions can be conservatively estimated to be in the thousands of calls per day. In fact, the investigation and prosecution of just one information broker company determined that company was making hundreds of calls daily. Remember, there are tens of thousands of information brokers, private investigators and collection agencies in the United States today. This means that it is very likely that your financial institution has already been the target of pretext calls.

The types of financial information advertised for sale include: individual and business bank account numbers and balances; individual and business bank account transaction records, including monthly statements; stock, bond and mutual fund holdings, including the number of shares held; insurance policy data, including the types of insurance maintained and the amount or value of the policy; credit card information, including account numbers, size of credit lines; and transaction details, including specific purchases.

Today there are literally dozens of information brokers and private investigators advertising their ability to locate financial institution customer account information in the United States by means of the World Wide Web. Using just one of numerous Internet search engines, anyone can locate a website advertising the sale of financial institution customer account information. The advertisements almost uniformly refer to "bank account searches" and/or "asset investigations." Not all of these firms are using pretext or violating the law, but investigations by state and federal authorities and the media have determined that many firms are in fact using pretext to gain customer information.

The financial services industry can address the threat by enacting security procedures designed to thwart pretext. The key is to balance customer information convenience with customer information security. By educating both financial institution employees and customers about the need for information security, the financial services industry will continue its leadership role in safeguarding customers' assets and information.


Pretext Methods

The four steps used by a pretext caller are:

1. Decide what information is sought;

2. Identify the custodian of the information;

3. Identify who the custodian will release the information to and under what circumstances; and

4. Use a pretext to be that person under those circumstances.

There are a variety of pretext methods in use today, and the list continues to grow. Numerous books and training courses are available to those seeking to use pretext to gain unauthorized access to confidential information. Additionally, on a daily basis, new pretext methods and variations are traded in Internet discussion areas specializing in pretext and investigation.

While pretext methods vary, all pretext calls to the financial services industry have one common feature: the individual illegally attempting to access customer information by placing a pretext call will try to convince the financial institution that the pretext caller is authorized to access the customer information.
In order to determine what pretext methods have the potential to defeat the institution's customer information security procedures, the institution must first determine what individuals and/or entities are currently granted access to customer information and under what circumstances. Once a list is created of who has access to customer information and under what circumstances that access is granted, an institution can make educated decisions concerning what methods of pretext might succeed in defeating the current customer information security procedures. Further, the institution can take steps to further review and strengthen procedures for access to customer information. Remember that a pretext caller failing to get the desired information from one employee will often call employee after employee, using the same or different methods. Traditionally, pretext callers have succeeded in using the following five general pretext methods to circumvent the customer information security procedures of a financial institution:

1) Impersonating a Customer. The most common pretext is the impersonation of a customer of an institution. The pretext caller will falsely state that he/she is the customer of the institution and needs to gain access to his/her account information. The pretext caller will often have the correct biographical information (name, address, phone number, date of birth, social security number) of the true account holder, having obtained this biographical information from public resources, proprietary investigative databases and identity theft.

However, in most pretexts the caller will be missing one or more pieces of information that are normally available to identify the caller as the account holder or that the institution requires in order to gain authorized access to account information. The most common missing pieces of information are account number; personal identification number (PIN); password; mother's maiden name; amount or date of last deposit or withdrawal; the branch or address of the institution where the account was opened; or the date when the account was opened.

The pretext caller will attempt to convince the financial institution that there is a reason the caller does not have the needed information; that the pretext caller is in fact the customer; and that the institution should bend the rules and allow access to account information because there is a compelling reason to do so. Typical examples of reasons given may include:

- "I don't have my account number because I don't have my check book with me here at work."
- "I can never remember that stupid PIN—I haven't had to use it for the longest time."
- "My mother's maiden name is Smith." (When informed that the name on record is different) Who are you to tell me what my mother's maiden name is? You must have written it down wrong on your end."
- "Password? I can't remember my password and I need this information right away or I'm going to start bouncing checks! Either give me my account information or I'm closing the account."
- "I don't have my account ledger here with me so how can I tell you my last deposit or withdrawal? Besides, my wife makes deposits and cashes checks all the time."
- "Please—it has been so long since I opened the account I can't remember where or when it was."

Examples of Other Pretexts that are Considerably More Elaborate Include:

- "I'm on a business trip and don't have my checkbook with me. I need to check my account balance in order to determine that a deposit was made so I don't bounce any checks. My mortgage check is in jeopardy of bouncing so you must help me."
- "I need to wire a large deposit to your customer, and the wire must happen today. Your customer is at the funeral of his mother, and I can't reach him. He gave me his account number but it got wet, and I can't read it. He needs this money to cover funeral expenses. You have to help me. I'll be sure he knows what great assistance you provided in his hour of need."
"I'm at the office and don't have my checkbook with me. I need to finish this car loan application and fax it in today. Can you please help me?

I need my account number and balance right away, or I won't be able to get this loan and close the deal."

"My wife and I separated several months ago, and she hasn't been forwarding my mail. I need to balance my account so I don't write any bad checks. I need you to fax the most recent copy of my statement to me here at the office."

Often, the goal of the pretext is to obtain information one piece at a time. Once the pretext caller finds an employee who will assist with one piece of information (which may not even be account specific) the pretext caller will continue to ask questions to try to obtain all the information necessary to access the account.

2) Impersonating Another Official within the Institution. If a pretext caller has difficulty bypassing the customer information security procedures of an institution by impersonating the customer, the caller may attempt to impersonate another employee or official of the institution. Remember that step three of a successful pretext is identifying whom the financial institution will release the information to and under what circumstances. An employee will almost always respond to the request of an individual the employee believes to be their superior within the institution. Institutions with more than one branch or physical location have employees who do not know everyone within the employ of the institution. This makes an internal pretext possible.

Examples of this Form of Pretext in the Financial Services Industry Include:

"Hi. This is Ann in Legal. I'm filling in today for Tracy and need to obtain some account information on John Jones. I have his social security number but can't figure out how to locate his information here on the computer. Everyone else is at lunch, and I need this right away. Can you help?"

"This is Bob with Customer Service over at the Park Avenue Branch. Our system just went down, and I have a distressed customer sitting in front of me that I need to help. Can you punch him up on your end and read me the following…"

3) Impersonating Another Institution. Another pretext that has been used with success for many years has been the impersonation of an employee of a separate institution. Many information brokers and identity thieves have learned that by posing as an official from another financial institution with questions concerning a customer they can successfully perform a pretext on the customer’s institution. This method takes advantage of the natural inclination to assist another institution in day-to-day activities. Often in this method a false story will be developed to elicit the help of the institution in stopping a fraudulent transaction. The goal is to appeal to the good nature of the employee to assist in stopping the fraud.

Examples of this Form of Pretext in the Financial Services Industry Include:

"Hi. This is Joe Jones over at Main Street Bank. Bob Smith, a customer of yours over there at 1st National Bank was in earlier and presented us with a check of yours that we had doubts about. Instead of completing the transaction, Mr. Smith walked out and said he would be back later. Can you bring up his account information and assist me in case he returns? We made a photocopy of the check before he left but the quality of the copy is poor, and we cut off the bottom so I don't have his account number. I have his full name and address if that helps…"

"Hi. This is Mary at Check Systems Fraud Department. We have some questions pertaining to a customer of yours…"

"Hi. This is Bob with Sears Credit Card Collection and Skip Trace Department. It appears we have a mutual customer in John Jones. I need some information from you regarding his account and in return I may be able to alert you to some irregular financial activity on his part…"
4) Impersonating a Government Regulatory Agency. While far less common, there are cases of pretext callers impersonating officials of government regulatory agencies. This form of pretext relies upon the recipient of the pretext call believing that the caller is an official needing access to customer information as part of an inquiry or investigation. Agencies reported to have been both impersonated and the recipients of pretext calls include the Federal Reserve, Federal Deposit Insurance Corporation and the Internal Revenue Service.

Remember that federal laws such as the Right to Financial Privacy Act prohibit the dissemination of information to government agencies by an institution unless there has been a search warrant, subpoena or administrative summons. Most government agents will understand your reluctance to provide such information over the phone.

5) Impersonating Law Enforcement Authorities. A final method that is used is the impersonation of law enforcement authorities. Similar to Pretext Method #4 above, this form of pretext again relies upon the reality that many financial institution employees will assist someone in law enforcement. This pretext has worked even when institutions have strict guidelines that notify employees they are not to release information absent a subpoena or other form of court order. A call from a purported police officer or Secret Service agent in need of immediate assistance can be very unnerving to an employee and can prey upon the employee's desire to assist law enforcement in preventing or solving a crime. Private investigators and private detectives have known for years that even when they properly identify themselves, whether by phone or in person, they are often mistaken for law enforcement officers. Unfortunately, there are unscrupulous private investigators and private detectives that have learned that by dropping the term "private," or by overtly misrepresenting themselves as law enforcement personnel, they increase the likelihood of obtaining the information they seek.

Examples of this Form of Pretext in the Financial Services Industry Include:

- "This is Investigator Jones. I need assistance with a matter I'm working on that involves one of your customers. I need you to assist me with a quick piece of information."
- "This is Detective Smith. We have your customer Mr. Jones in custody, and I need to verify his account number and balance. Mr. Jones is in the lock-up and claims he doesn't remember his account number. I have his social security number and address if that will help you find the account."

Spotting Pretext Calls

There are a number of indicators that what at first appears to be a routine and valid request for customer information may instead be a pretext call. The presence of any one of these indicators or a combination thereof does not always indicate a pretext attempt. Financial institutions receive numerous requests every day for customer information. In many of those requests one or more of the following indicators may be present and be perfectly innocent. However, financial institution employees should be aware of these potential indicators and review them on a regular basis in order to be prepared to spot a potential pretext.

Most important, remember that the pretext caller is a confidence artist. The basis of the confidence game for the pretext caller is to take advantage of the financial services industry's reputation as customer service-oriented. By appealing to the emphasis placed on customer service within the industry, the pretext caller attempts to obtain information that he or she is not legally entitled to. If it feels like a con – it probably is.

Missing Information: Any call or request for customer information where the institution's defined requirements for gaining access (PIN, password, last date of deposit and amount, etc.) are not met.

Non-customer Calls: Any call where the person requesting the information is not the customer.

Calls Placed from Numbers Others Than Those Listed on the Customer's Account: If an institution has caller identification capabilities, employees should note whether the phone number displayed matches the phone number(s) associated with the customer account. Particular attention should be given to calls
placed from outside the local calling area of the customer and calls that have been placed that block the caller identification feature.

**Callers Who are Hesitant or Refuse to Give a Call-back Number:** Any caller that refuses or hesitates in providing the number they are calling from may be concerned about the call being traced back to them. Many pretext callers will immediately hang up if confronted with a courteous request for the number they are calling from.

**Out of the Ordinary Request:** Any call that is out of the ordinary. This includes requests for faxes of account information or statements to numbers outside the local calling area of the customer and requests to mail duplicates of account information to an address other than that on the customer account.

**Overly Aggressive Callers:** Any caller who becomes belligerent or aggressive when asked routine account identifying information. A favorite ploy of pretext is to bully the employee into releasing information by threats to speak to a supervisor, close an account or make a complaint about the employee.

**Overly Talkative Callers:** Callers who appear to be laying out a story concerning why they need to bypass the access rules of the institution or who appear to be attempting to distract the employee with excessive chit-chat while posing more account-related questions may be constructing a pretext. The best pretexts lure the employee into providing information not even requested in an attempt to assist the confused caller.

**Absentminded Callers:** Callers who appear to be overly confused or absent-minded and are unable to provide even basic biographical information may be placing a pretext call. Many pretexts rely on placing many calls to the institution and picking up one piece of information at a time until enough data are collected to convince the institution that the caller is the legitimate account holder.

**Handling a Possible Pretext Call**

All financial institutions should develop policies and guidelines for employees to follow when a pretext call is suspected. It must be stressed that the policies and guidelines are to be followed without exception by all employees of the institution. Considerations for policies and guidelines should include:

**No Variation From Customer Information Access Procedures:** Whatever customer information access procedures are determined to be appropriate for the individual institution should be strictly enforced. No frontline employee should have the authority to deviate from the stated procedures. Legitimate customers will appreciate security procedures when it is explained that the procedures are in force to protect their valuable information. Frontline employees should be instructed that they could be dismissed from their job for deviating from the institution's customer information security procedures.

**Routing Suspected Pretext Calls to a Supervisor Or Security Official:** Any suspected pretext call should be brought to the immediate attention of a supervisor or security official within the institution and if feasible the call should be routed to that official. Many pretext attempts will end with a hang-up by the pretext caller as soon as a transfer to another official begins. Many pretext callers would prefer to end the call and try again at a later point than deal with a supervisory or security official.

**Recording Suspected Pretext Calls:** Where applicable state and federal laws permit, consideration should be given to recording any suspected pretext calls. Several successful prosecutions of pretext callers have been based upon recorded attempts at gaining access to customer information.

**Notation Of Suspected Pretext Calls:** At all times employees should make note of any suspected pretext call. If possible, notation should be on the individual account so that, if further attempts to gain access occur, other institution employees will be aware of the history of pretext attempts on the account. The notes should include the method of the suspected pretext. Pretext callers will repeatedly call an institution and speak with different employees until they gain access.

Notes on the account of attempted access can serve to notify other employees to give the account special attention.
Request A Call-back Number: Requesting a call-back number will often assist in determining if the call is a pretext. Many pretext callers will immediately hang up when asked to provide a call-back phone number. If the number does not match the phone numbers associated with the account, ask the caller where they are and who is the owner of the call-back phone number. Most legitimate callers will not mind providing that information and will be impressed with your security efforts on their behalf.

Stopping Pretext Calls

As part of an overall security plan, consider the following elements covering pretext call prevention:

Customer Information Security Plan: The plan should address the threat of pretext calls to the integrity of a customer's personal information and the reputation of the institution. You should determine who currently has authority to release information and under what circumstances the release can be made. Check that your procedures are consistent with current practice.

Do Not Deviate from Customer Information Security Procedures: Once a comprehensive plan has been developed it must be adhered to uniformly. Supervisors should demonstrate to frontline personnel that they take the procedures seriously by both following the procedures and enforcing them.

Use Authorization Codes or Passwords: Codes, passwords or other identifying information should always be used before any release of information by phone, fax or other telecommunication device.

Refer Questionable Calls to a Supervisor or Security Official: A supervisor or security official should handle all calls that are questionable or suspicious. The act of routing a call to a supervisor or security official will deter most pretext callers for fear of further scrutiny of their actions. Legitimate customers will appreciate the attention being provided to maintaining the integrity of their account.

Educate Employees: All employees are potential targets of pretext calls and should receive regular and repeated training to identify and handle pretext calls in conformity with your information security procedures.

Test Your Customer Information Security Procedures: Internal or third-party pretext testing should routinely evaluate your information security procedures. This will help identify weaknesses in procedures or training.

Educate Customers: Educate customers about the high degree of emphasis you place on protecting this information. Remind customers that they should never provide their customer information to anyone over the phone unless they initiated call and are certain with whom they are dealing. When dealing with a difficult customer who wants access to information but is unable to provide appropriate identification, stress that the procedures of the institution are designed to protect their assets from identity thieves.

Report Suspicious Advertisements by Information Brokers, Private Investigators, Collection Agencies and Others: Look for advertisements in local publications, trade journals, magazines, yellow pages and on the Internet referring to the ability to locate “assets.” Pay particular attention to advertisements claiming to be able to locate account, credit card, stocks, bonds, mutual funds and insurance information. Users of pretext are notorious for claiming that they follow all laws and require appropriate documentation. Report suspicious advertisements to local and federal law enforcement and regulatory bodies including the Federal Trade Commission.

Report Pretext Attempts to the Appropriate Authorities: If you determine that a pretext caller is targeting your institution, you should contact your regulator or, if you believe that the pretexting is being done to commit a fraud, consider filing a Suspicious Activity Report (SAR) with the Treasury's Financial Crimes Enforcement Network. While the filing of a SAR is not required, the agencies may issue a guidance encouraging the filing if a potential identity theft is involved. You may also wish to contact the FTC, which is keeping information on identity theft cases, at 1-877-IDTHEFT. Prosecution can also be an effective deterrent. For example, most information brokers and private investigators are refusing to accept asset investigations in the State of Massachusetts because of the State’s aggressive prosecution of pretext callers.
Tool 7: Communicating Your Security Practices

Financial institutions have always valued the trust customers have that we will protect their personal financial information. Communicating what you do in the way of protecting customer information is where your security and your privacy responsibilities under the Gramm-Leach-Bliley Act intersect.

Your institution’s privacy policy is but one place where you can talk to your customers and other stakeholders about your security initiatives. Other opportunities exist, and you should consider taking advantage of them to demonstrate how seriously you view the issue. It is also important to provide your customers with the tools to protect themselves, particularly from identity theft. Empowering your customers with the tools to protect themselves solidifies the partnership that your institution and your customers have to mutually safeguard their financial information. This tool is designed to assist your institution in building that partnership.

Security and Your Privacy Policy

Security is an integral part of your privacy policy and your privacy policy should describe in general terms how you protect customer information. The following samples of security language are examples of how other institutions have incorporated their security measures into their privacy policy.

SAMPLE 1:

The security of the communications between you and our servers is ensured using cryptography, which scrambles messages exchanged between your browser and our online banking server. When you go to the sign-on page for online banking, your browser establishes a secure session with our server. The secure session is established using a protocol called Secure Sockets Layer (SSL) Encryption. The SSL protocol, not only ensures privacy, but also ensures that no other browser can "impersonate" your browser, nor alter any of the information sent. You can tell whether your browser is in secure mode by looking for the secured lock symbol at the bottom of your browser window.

It is also important to verify that only authorized persons log into home banking. This is achieved by verifying your password. When you submit your password, it is compared with the password we have stored in our secure data center. We allow you to enter your password incorrectly five (5) times. If you enter your password incorrectly five times, your online banking account will be locked until you call us to reinitialize the account. We monitor and record "bad-login" attempts to detect any suspicious activity (i.e., someone trying to guess your password). You play a crucial role in preventing others from logging on to your account. Never use passwords that are easy to guess. Examples of bad passwords are: Birth dates, first names, pet names, addresses, phone numbers, social security numbers, etc. Never reveal your password to another person. You should periodically change your password in the User Option screen of online banking.

SAMPLE 2:

Our Internet Banking System brings together a combination of industry-approved security technologies to protect data for the bank and for you, our customer. It features password-controlled system entry, a Identrus-issued Digital ID for the bank’s server, Secure Sockets Layer (SSL) protocol for data encryption, and a router loaded with a firewall to regulate the inflow and outflow of server traffic.

Secure Access and Verifying User Authenticity

To begin a session with the bank’s server the user must key in a Log-in ID and a password. Our system, the Internet Banking System, uses a "3 strikes and you’re out" lock-out mechanism to deter users from repeated login attempts. After three unsuccessful login attempts, the system locks the user out, requiring either a designated wait period or a phone call to the bank to verify the password before re-entry into the system. Once the server session is established, the user and the server are in a secured environment, ensuring the secure transfer of data.
Router and Firewall

Requests must filter through a router and firewall before they are permitted to reach the server. A router, a piece of hardware, works in conjunction with the firewall, a piece of software, to block and direct traffic coming to the server. The configuration begins by disallowing ALL traffic and then opens holes only when necessary to process acceptable data requests, such as retrieving web pages or sending customer requests to the bank.

SAMPLE 3:

Our Bank is dedicated to the protection of its customers' privacy. All personal and financial information submitted through the Our Bank website will be kept accurate, secure and confidential. We maintain security standards and procedures to help prevent unauthorized access to confidential information about you. Our Bank's secure network will recognize communications from customers using browsers that are compliant with certain security standards. If you are using Netscape Navigator 3.0 or higher, Microsoft's Internet Explorer 3.0 or higher or any other SSL compliant browser, you may submit applications/requests for information online.

Cookies

Once a customer has signed into the Internet Banking service and his or her User ID and password have been validated, session management information that is stored on the customer's PC is maintained. This encrypted data element helps an authenticated customer navigate the web site. This data element, called a "cookie," is stored in the computer browser's memory. This cookie exists only in the memory of the browser and is active only as long as the customer's browser is running or until the time out limit has been reached. Once the browser is closed or timed out, the information is deleted. A cookie does not retrieve data from your hard drive, carry computer viruses, or capture your e-mail address. Most browsers will allow you to disable cookies or warn you before accepting a cookie. However, if you decide not to accept cookies, you may not be able to successfully navigate within the Internet Banking service.

SAMPLE 4:

Security of your account is our number one priority. With online banking, you can do your banking with confidence. We use state-of-the-art technology and a combination of security measures to make your banking sessions secure.

Bank-Approved Browsers

Our standards are among the highest of companies on the Internet. We require that you use a current version of a browser that supports 128-bit encryption and SSL3, the highest level of encryption commercially available. We do not allow any information from your banking session to be stored on your hard drive unless you download it and save it on your computer.

Password and PIN

You will need to authenticate yourself each time you use online banking by entering in your user name and password (selected at enrollment) plus your Card number and PIN. Together, this serves as your unique access to Online Banking. You should never disclose your password or PIN to anyone, including anyone claiming to represent our Bank.

Preventing Unauthorized Use

Our Bank uses firewalls to prevent anyone without proper authorization from accessing online banking. A firewall also regulates information coming in and going out, making sure that communications happen only between approved parties.
Timed Log Out

If you leave your computer unattended, or go to another Web site without logging out, we will automatically end your banking session after 10 minutes of inactivity.

SAMPLE 5:

This Internet Banking System brings together a combination of industry-approved security technologies to protect data for the bank and for you, our customer. It features password-controlled system entry, a VeriSign-issued Digital ID for the bank's server, Secure Sockets Layer (SSL) protocol for data encryption, and a router loaded with a firewall to regulate the inflow and outflow of server traffic.

Secure Access and Verifying User Authenticity

To begin a session with the bank's server the user must key in a Log-in ID and a password. Our system, the Internet Banking System, uses a "3 strikes and you're out" lock-out mechanism to deter users from repeated login attempts. After three unsuccessful login attempts, the system locks the user out, requiring either a designated wait period or a phone call to the bank to verify the password before re-entry into the system. Upon successful login, the Digital ID from VeriSign, the experts in digital identification certificates, authenticates the user's identity and establishes a secure session with that visitor.

Secure Data Transfer

Once the server session is established, the user and the server are in a secured environment. Because the server has been certified as a 128-bit secure server by VeriSign, data traveling between the user and the server is encrypted with Secure Sockets Layer (SSL) protocol. With SSL, data that travels between the bank and customer is encrypted and can only be decrypted with the public and private key pair. In short, the bank's server issues a public key to the end user's browser and creates a temporary private key. These two keys are the only combination possible for that session. When the session is complete, the keys expire and the whole process starts over when a new end user makes a server session.

Router and Firewall

Requests must filter through a router and firewall before they are permitted to reach the server. A router, a piece of hardware, works in conjunction with the firewall, a piece of software, to block and direct traffic coming to the server. The configuration begins by disallowing ALL traffic and then opens holes only when necessary to process acceptable data requests, such as retrieving web pages or sending customer requests to the bank.

Using the above technologies, your Internet banking transactions are secure.

Going Beyond GLB: Medical Privacy and Identity Theft

Identity Theft Prevention and Resolution Self-Assessment

The following questionnaire has been developed in order to improve your customers’ ability to avoid becoming victimized by identity theft and to assist customers who have been affected by that crime. Review your procedures as you respond to these questions and consider modifications where appropriate.

Research

Find out how much money your institution lost in account takeover and fraudulent applications. The ABA's 1998 Check Fraud Survey found that $3 out of every $4 dollars lost by a community bank to check fraud was due to some form of identity theft.
Review

Review your authentication processes and policies regarding access to data. Are they effective in helping spot and handle pretext calls? Tool 5's pretext calling materials can help in a number of these areas.

Handling Customer Calls

- Do you have a central number for ID theft questions/calls?
- What advice do you give a customer when he or she calls and claims someone stole his or her identity? **Beware, some calls may be pretext calls!**
- Do you provide customers with a victim's kit, including an affidavit, control form, letters to bureau, creditor, etc. ABA's *Identity Theft Communications Kit* has the elements for developing your own victim's kit.
- Do you advise customers to file a police report? Does your institution file a Suspicious Activity Report?
- Who is monitoring timely responses to disputes, including investigation (e.g., compliance officer, security officer, customer service representative supervisor)?

Internal Procedures

- Are customer contact areas equipped to respond to customer ID theft issues?
- Do you provide your fraud/customer service areas with ID theft "red flags"?
- Within your institution, do you share fraud alerts across your various lines of businesses?
- When a customer advises your institution that his or her account was stolen, do you close the account immediately and issue a new card or new checks?
- What are your procedures surrounding change of address? Do you:
  - Verify customer information prior to executing the address change?
  - Confirm change at both addresses?
- What is the process for new check/card requests?
  - Do you notify customers of such requests made 30 days after address change?

Train

Provide general training on keeping information confidential. See Tool 5: Training Your Employees for a manual on spotting and avoiding pretext calls. Also, last year ABA offered to members a privacy awareness video entitled Consumer Privacy Training Video. If you have not yet ordered your copy (the first is free to ABA members), please call 1-800-BANKERS.

Communicating with your customers is vital to preventing identity theft. ABA's Identity Theft Communications Kit — which was sent to ABA members in July — will help you to do this and position your
institution as a partner in privacy with your customers. The kit contains ideas on both the prevention and resolution side, including:

<table>
<thead>
<tr>
<th>Prevention</th>
<th>Resolution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Consumer Tips</td>
<td>Steps to Take for Victims</td>
</tr>
<tr>
<td>Sample Speech</td>
<td>Sample Letter to Customers</td>
</tr>
<tr>
<td>Radio Script</td>
<td>Customer Account Record Worksheet</td>
</tr>
<tr>
<td>Sample Press Release</td>
<td>Customer Activity Log</td>
</tr>
<tr>
<td>Media Talking Points</td>
<td></td>
</tr>
<tr>
<td>Sample Advertisement</td>
<td></td>
</tr>
<tr>
<td>Sample Newsletter Article</td>
<td></td>
</tr>
</tbody>
</table>

ABA members may obtain an additional copy of the Identity Theft Communications Kit by visiting our website at [http://www.aba.com/](http://www.aba.com/) or by calling 1-800-BANKERS.

**Going Beyond GLB: Medical Privacy and Identity Theft**

**Simple Steps to Safeguard Your Identity**

*Print this article in your customer or employee newsletter.*

Up to 500,000 individuals are victims each year of identity theft, a fast-growing form of fraud. Fortunately, a few simple steps can help ensure you stay out of these statistics.

"Identity theft" or "account takeover fraud" involves criminals stealing a person's personal information. The crooks assume a person's identity, apply for credit in his or her name, run up huge bills, stiff creditors and generally wreck the victim's credit record.

At [institution name], we put a combination of safeguards in place to protect customers, including employee training, rigorous security standards, data encryption and fraud detection. You can take these steps to avoid becoming a victim:

- Don't give your Social Security or account numbers to anyone over the phone unless you initiated the call.
- Tear up receipts, old account statements and unused credit card offers before throwing them away. Crooks could steal information from your trash and use it to get credit in your name.
- Review your account and credit card statements as soon as you receive them to check for unauthorized transactions.
- Protect your PINs and computer passwords; use a combination of letters and numbers and change them often. Never carry this information with you!
Order copies of your credit report once a year to ensure accuracy. Call any of the three national credit reporting agencies: Trans Union (800) 888-4213, Equifax (800) 685-1111 and Experian (888) 397-3742.

Report any suspected fraud to your bank and credit card issuers immediately so they can start to close accounts and clear your name right away.

By law you are only liable for the first $50 of unauthorized charges against a credit card account. Still, restoring your identity can be a tremendous inconvenience. It's worth your while to exercise a little preventive maintenance. Protect yourself against this terrible crime.

For more personal finance tips, visit our Web site at [Web address] or visit the American Bankers Association's Consumer Connection at http://www.aba.com/.

**Going Beyond GLB: Medical Privacy and Identity Theft**

**Steps to Take if You are a Victim of Identity Theft**

*Publish these steps on your bank letterhead for any customers that come to your bank for help.*

If you suspect misuse of your personal information to commit fraud, **take action immediately.** Keep a record of all conversations and correspondence when you take the following suggested steps:

1) **Contact your financial institutions & credit card issuers immediately** so that the following can be done: access to your accounts can be protected; stop payments on missing checks; personal identification numbers (PINs) and online banking passwords changed; and a new account opened, if appropriate. Be sure to indicate to the financial institution or card issuer all of the accounts and/or cards potentially impacted including ATM cards, check (debit) cards and credit cards. Customer service or fraud prevention telephone numbers can generally be found on your monthly statements. Contact the major check verification companies to request they notify retailers using their databases not to accept these stolen checks, or ask your bank to notify the check verification service with which it does business. Three of the check verification companies that accept reports of check fraud directly from consumers are: Telecheck (800) 710-9898, International Check Services (800) 631-9656 and Equifax (800) 437-5120.

2) **File a police report** with your local police department. Obtain a police report number with the date, time, police department, location and police officer taking the report. The police report may initiate an investigation into the loss with the goal of identifying, arresting and prosecuting the offender and possibly recovering your lost items. The police report will be helpful when clarifying to creditors that you are a victim of identity theft.

3) **Contact the three major credit bureaus** and request a copy of your credit report. Review your reports to make sure additional fraudulent accounts have not been opened in your name or unauthorized changes made to your existing accounts. Check the section of your report that lists "inquiries." Request the "inquiries" be removed from your report from the companies that opened the fraudulent accounts. In a few months, order new copies of your reports to verify your corrections and changes to make sure no new fraudulent activity has occurred. Request a "fraud alert" for your file and a victim's statement asking creditors to call you before opening new accounts or changing your existing ones. This can help prevent an identity thief from opening additional accounts in your name. Here are the major credit bureaus and their phone numbers: Equifax (800) 525-6285, Experian (888) 397-3742 and Trans Union (800) 680-7289.

4) **Check your mailbox** for stolen mail. Make sure no one has requested an unauthorized address change, title change, PIN change or ordered new cards or checks to be sent to another address. If a thief has stolen your mail to get credit cards, bank and credit card statements, pre-screened credit offers or tax information, or if an identity thief has falsified change-of-address forms, that's a crime. Contact your local post office and police.

5) **Maintain a written chronology of what happened,** what was lost and the steps you took to report the incident to the various agencies, financial institutions and firms impacted. Be sure to record the date, time,
ABA Identity Theft Communications Kit
Prevention & Resolution

Use this ABA Communications Kit -- specially designed for ABA members only -- to help educate customers on identity theft and how they can protect themselves in the Information Age:

- Identity Theft Communications Kit (PDF)
- Identity Theft Customer Account Record (PDF)
- Identity Theft Customer Activity Log (PDF)
- Identity Theft Affidavit (Federal Trade Commission)

Contents of the Identity Theft Communication Kit available in HTML format include:

- Letter from ABA President Hjalma Johnson
- Sample Press Release
- Media Talking Points
- Sample Advertisement
- Sample Employee Memo
- Sample Newsletter Article
- Consumer Tips
- Sample Speech
- Radio Script
- Victims: Steps to Take
- Sample Customer Letter

Questions? Please contact Doug Adamson at 202-663-5360 or by email at dadamson@aba.com for further information.