CERP Exam Content Outline

Reference Resource

SECTION 1 – RISK GOVERNANCE

Domain 1: Board and Senior Management Oversight | 8%

Task 1: Provide relevant, timely, and accurate information to board, risk committees, and senior management.

Knowledge of:

a. Organizational structures and committees and their roles and responsibilities (e.g., governance, credible challenge)
b. Processes to manage and report the status of risk identification, measurement, and control activities
c. The concepts and components of risk appetite and risk culture and how they link to corporate strategy and operations

Task 2: Champion policies, risk appetite, and risk culture across the organization.

Knowledge of:

a. Practices to drive organizational, process, and cultural change (e.g., communicating expectations, define roles) in alignment with business objectives and strategy
b. The concepts and components of risk appetite and risk culture
c. How risk appetite and risk culture link to corporate strategy and operations
d. Practices to educate and increase awareness of risk policies, appetite, and culture within and across all three lines of defense

Domain 2: Policies, Procedures and Limits | 12%

Task 1: Establish and maintain risk management policies, procedures, and risk appetite framework in alignment with enterprise objectives.

Knowledge of:

a. Elements of an effective control environment (e.g., policy review/governance)
b. Regulatory expectations around policies (e.g., proper authority, breadth of coverage, approval)
c. Methods to implement and communicate risk management policies
d. The concepts of organizational control structure and escalation channels
e. Risk management policies' purpose, roles, and responsibilities
f. The components of risk appetite (e.g., qualitative, quantitative) and how they link to corporate strategy
g. Assessment of risk appetite levels and monitoring thresholds
h. Regulator expectations of procedures to execute in alignment with risk management policies

Task 2: Establish a governance process to create and maintain policy limits for measuring business performance.

Knowledge of:

a. Development and maintenance of policy limits (e.g., setting appropriate limits, periodic review expectations)
b. Calculation of risk metrics/quantitative methods
c. Typical sources of risk concentration (e.g., portfolio concentration, uninsured deposits, counterparty)

Task 3: Manage policy exceptions (e.g., LTV exception) and policy breach (e.g., data privacy breach).

Knowledge of:

a. Documentation of policy exceptions
b. Appropriate approval authority used for exception
c. Establish timelines and processes for noncompliance to policy for decision-making (e.g., exceptions, risk mitigation, dispensation)
d. Process and requirements for breach in policy (e.g., escalate, document, track)

Domain 3: Management Information Systems | 11%

Task 1: Develop and maintain management information systems (i.e., reporting tools) to systematically track and evaluate the effectiveness of the risk management program.

Knowledge of:

a. Risk aggregation analysis tools and processes
b. System limitations (e.g., access restrictions, manual versus automated reporting)
c. Information systems and data required for risk reporting (e.g., asset liability systems)
d. Information collection, retention, and sharing (e.g., completeness, quality, accessibility)
e. Design elements in MIS reports to aid in effective decision-making

Task 2: Assess the quality and capabilities of the systems used to support the decision-making activities.

Knowledge of:

a. Industry standards, sound practices, and regulatory expectations regarding information systems related to enterprise risk management
b. Investigative approaches to ensure system function as expected (e.g., inquire, observe, request documentation, challenge)

Task 3: Develop and implement data governance program to ensure completeness and accuracy of reporting.

Knowledge of:

a. Fundamental system requirements (e.g., asset liability system, modeling, Credit Risk, risk assessment)
b. Methodologies for confirming and challenging the integrity of inputs and outputs (e.g., model validation, reconciliation)
c. Investigative approaches to ensure data is accurate and complete (e.g., inquire, observe, request documentation, challenge)
d. Controls for information systems providing data required for risk reporting (e.g., asset liability systems)
e. Quality control processes and accountability

Domain 4: Control Framework | 7%

Task 1: Determine if the internal control framework aligns with the size, complexity, and risk appetite of the organization.

Knowledge of:

a. Three lines of defense (e.g., roles, responsibilities, independence)
b. Internal control system (e.g., control environment, risk assessment, control activities)
c. Internal control framework (e.g., COSO Integrated Control Framework)
d. Regulatory requirements (e.g., Sarbanes-Oxley Act [SOX], Heightened Standards)
e. Control types (e.g., preventative/detective, manual/automated)
f. Effective challenge by risk management staff
g. Quality control and quality assurance
h. Effective controls for all risk categories (e.g., model risk, fraud, external financial reporting, Sarbanes-Oxley Act [SOX])

Task 2: Coordinate timing, coverage, and scope of risk management reviews with those of other control partners (e.g., independent risk, compliance) and prepare for regulatory exams.

Knowledge of:

a. The roles and responsibilities of the three lines of defense
b. Principles for effective exam management

SECTION 2 – RISK MANAGEMENT

Domain 5: Risk Identification | 15%

Task 1: Monitor and survey the internal and external environment to identify emerging risks.

Knowledge of:

a. Risk categories (e.g., Operational Risk, Credit Risk) and types of risk events (e.g., processing errors, loan default)
b. Potential upstream and downstream impact of risk events
c. Risk presented by third parties (e.g., concentration, financial health)
d. Criteria for materiality
e. Regulatory environment and industry trends

Task 2: Identify current risks through the development of risk and control self-assessment (RCSAs).

Knowledge of:

a. Risk categories (e.g., Operational Risk, Credit Risk) and types of risk events (e.g., processing errors, loan default)
b. Potential upstream and downstream impact of risk events
c. Risk presented by third parties (e.g., concentration, financial health)
d. Risk and control self-assessment (RCSA) fundamentals (e.g., inherent risk, residual risk, business processes)
e. Regulatory environment and applicable requirements

Task 3: Identify idiosyncratic risks (e.g., unique product lines, third-party relationships, customer concentration).

Knowledge of:

a. Risk categories (e.g., Operational Risk, Credit Risk) and types of risk events (e.g., processing errors, loan default)
b. Potential upstream and downstream impact of risk events
c. Criteria for materiality
d. Regulatory environment and applicable requirements

Task 4: Identify risks resulting from failure to meet internal and external stakeholder requirements.

Knowledge of:

a. Potential upstream and downstream impact of risk events
b. Criteria for materiality
c. Potential regulatory actions and penalties (e.g., Matters Requiring Attention [MRA], Civil Money Penalties [CMP])

Domain 6: Risk Measurement and Evaluation | 13%

Task 1: Estimate the likelihood of risk event(s) and the potential impact(s).

Knowledge of:

a. Risk assessment factors including likelihood, impact, direction, and velocity
b. Key indicators (e.g., KRI, KPI) across all risk categories
c. Evaluation of inherent risk, control environment, and residual risk
d. Development and calculation of risk metrics/quantitative methods
e. External factors (e.g., economic, regulatory, environmental)
f. Potential upstream and downstream impact of risk events
g. Effects of aggregated risks

Task 2: Conduct scenario analysis (e.g., stress test).

Knowledge of:

a. Scenario analysis fundamentals (e.g., scenario selection, triggers)
b. Regulator expectations for conducting scenario analysis (e.g., asset size, complexity)
c. Key indicators (e.g., KRI, KPI) across all risk categories
d. Calculation of risk metrics
e. Application and limitations of stress testing and scenario analysis
f. External factors (e.g., economic, regulatory, environmental)

Task 3: Complete risk and control self-assessments (RCSAs).

Knowledge of:

a. Risk assessment factors including likelihood, impact, direction, and velocity
b. Evaluation of inherent risk, control environment, and residual risk
c. Risk scoring and prioritization

Task 4: Evaluate risk relative to risk appetite and risk tolerance.

Knowledge of:

a. Key indicators (e.g., KRI, KPI) across all risk categories
b. Risk appetite and tolerance

Domain 7: Risk Responses | 18%

Task 1: Evaluate the alignment of management's risk response and documentation with risk appetite.

Knowledge of:

a. Types and examples of risk responses (i.e., accept, mitigate, transfer, avoid), and when each is appropriate
b. Maintenance of Risk and Control Self-Assessment (RCSA)

Task 2: Develop and recommend risk response (i.e., accept, mitigate, transfer, avoid).

Knowledge of:

a. Types and examples of risk responses (i.e., accept, mitigate, transfer, avoid) and when each is appropriate
b. Types of risk mitigation activity (e.g., preventative, detective, corrective)
c. Root cause analysis principles and techniques
d. Impact from internal and external risks (e.g., third-party service providers, shared services)
e. Risk appetite and tolerance

Task 3: Manage issues identified by the first line and second line.

Knowledge of:

a. Issues Management identification and tracking
b. Types and examples of risk responses (i.e., accept, mitigate, transfer, avoid) and when each is appropriate relevant to risk appetite
c. Root cause analysis principles and techniques
d. Impact from internal and external risks (e.g., third-party service providers, shared services)
e. Issues Management resolution (e.g., validation, closure)

Task 4: Respond to findings from regulators, independent third parties, and audits.

Knowledge of:

a. Root cause analysis principles and techniques
b. Methods to address findings (e.g., rating criticality, action plan, documentation, disposition)

Task 5: Determine the residual risk of an event post-risk response.

Knowledge of:

a. Evaluation of inherent risk, control environment, and residual risk
b. Maintenance of Risk and Control Self-Assessment (RCSA)

Domain 8: Risk Monitoring | 16%

Task 1: Identify and define key indicators (e.g., KRI, KPI).

Knowledge of:

a. Key credit measures (e.g., debt to income ratio, net credit losses, percentage of non-performance asset)
b. Key financial measures (e.g., net interest income, tier 1 capital ratio, current ratio)
c. Key non-financial measures (e.g., operational losses, system downtime, employee turnover, efficiency ratio)
d. Risk appetite and tolerance
e. Distinction between key indicators (i.e., performance vs. risk)
f. Indicators of economic trends (e.g., unemployment, bankruptcy rate)
g. Elements of effective risk measures (e.g., limit, trigger)

Task 2: Design and produce standardized and ad hoc reporting.

Knowledge of:

a. Report monitoring and distribution components (e.g., timeline, scoping, time horizon, level of aggregation, segmentation)
b. Techniques for analyzing risk information (i.e., quantitative, qualitative)
c. Methods to summarize and communicate risk information (e.g., color coding, heat mapping, dashboard)
d. The proper level to distribute and make information available, including escalation
e. Reporting requirements

Task 3: Monitor indicators and reports to identify emerging risks.

Knowledge of:

a. Report monitoring and distribution components (e.g., timeline, scoping, time horizon, level of aggregation, segmentation)
b. Techniques for analyzing risk information (i.e., quantitative, qualitative)
c. The proper level to distribute and make information available, including escalation
d. Key credit measures (e.g., debt-to-income ratio, net credit losses, percentage of non-performance asset)
e. Key financial measures (e.g., net interest income, tier 1 capital ratio, current ratio)
f. Key non-financial measures (e.g., operational losses, system downtime, employee turnover, efficiency ratio)

Task 4: Evaluate the quality of first line performance through control monitoring.

Knowledge of:

a. Report monitoring and distribution components (e.g., timeline, scoping, time horizon, level of aggregation, segmentation)
b. Control design and operating effectiveness
c. Techniques for analyzing risk information (i.e., quantitative, qualitative)
d. The proper level to distribute and make information available, including escalation
e. Reporting requirements

Task 5: Analyze report output and make risk-based recommendations.

Knowledge of:

a. Methods to summarize and communicate risk information (e.g., color coding, heat mapping, dashboard)
b. Techniques for analyzing risk information (i.e., quantitative, qualitative)
c. The proper level to distribute and make information available, including escalation