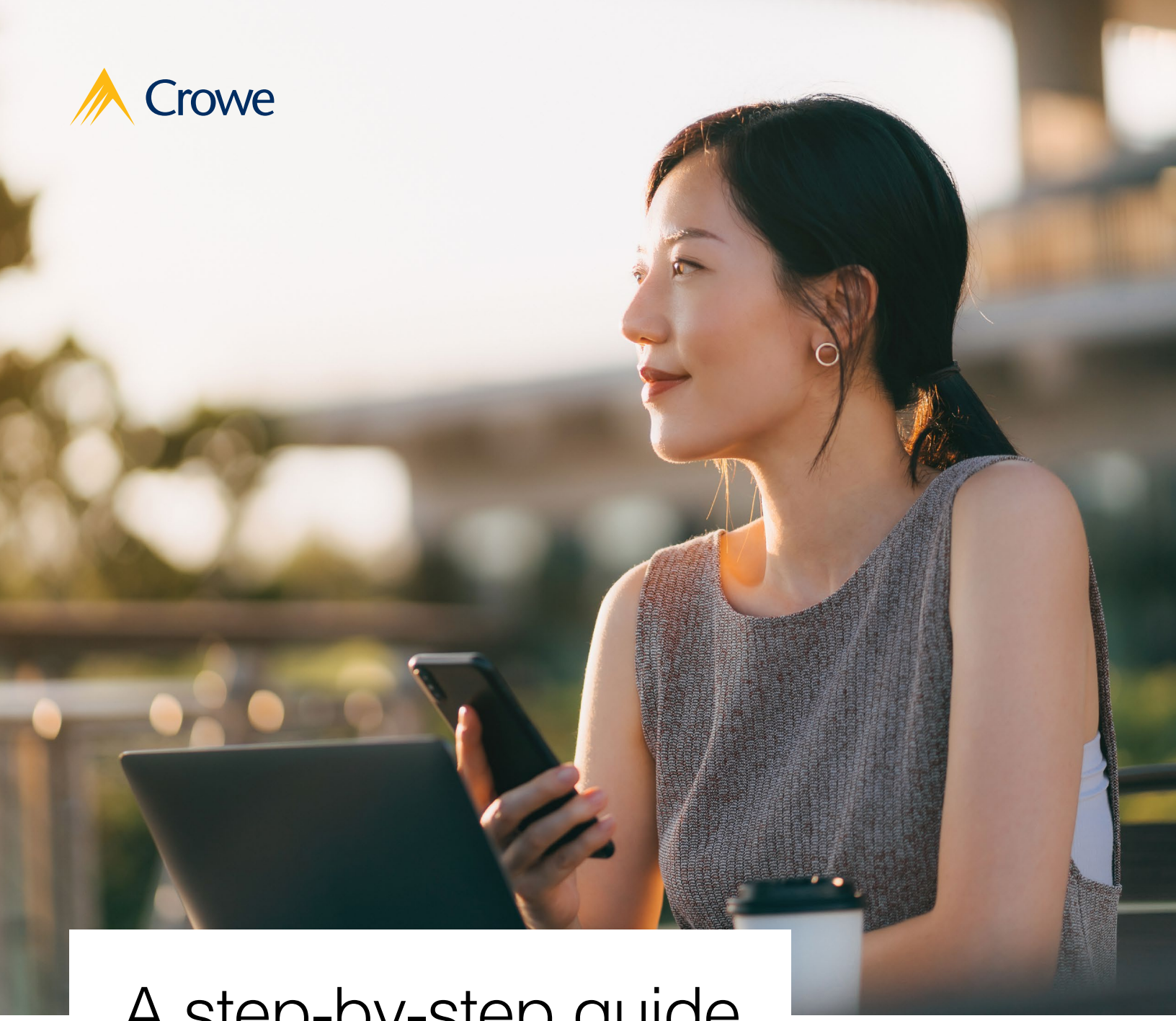
Crowe



A step-by-step guide

Implementing MFA in financial services

Given increasingly sophisticated cyberthreats, **the old login practice of username and password isn't enough.**

Multifactor authentication (MFA) is the new standard, and financial services organizations should prepare for MFA adoption.

What is multifactor authentication?

Multifactor authentication is a security system that requires users to provide more than just a username and password to verify their identity for a login or other transaction. To receive access, users must provide:

Something they **know** → Something they **have** → Something they **are**

A knowledge factor, such as a password or PIN

A possession factor, like an ID card or code from their mobile device

An inherence factor, like a fingerprint or recognition of their voice

Why should our organization implement MFA?

In the financial services sector, security is paramount. According to a February 2022 survey by VMware, 63% of financial services organizations reported an increase in destructive attacks within the past year – a figure that rose 17% from the previous year's survey. With the increasing number of cyberthreats, financial services organizations must heighten their efforts to secure their customers' data and funds.

MFA provides an additional layer of security that makes it harder for attackers to gain access to a person's devices or online accounts since knowing the victim's password alone is not enough to pass the authentication check.

What challenges should we expect when implementing MFA?

While MFA provides an additional layer of security, it also comes with its own set of challenges.

Challenge	Solution
Users experience inconvenience or frustration due to the additional authentication step.	Choose an MFA solution that's easy to use and provide adequate training for users.
MFA implementation can incur significant upfront costs, especially for large organizations.	Follow a detailed and proven methodology for MFA implementation. Also, when evaluating MFA costs, consider the cost savings achieved by preventing potential future security breaches.
Implementation of MFA can raise technical challenges, especially when integrating with existing systems.	Select an MFA solution that's compatible with existing systems and employ a skilled technical team to implement that solution.

01 4 steps for a successful financial services MFA rollout

A successful MFA rollout requires clarity in terms of goals, expectations, and timelines. Without thorough planning, proper training, and clear communication, it could devolve into an avalanche of employee complaints and IT requests.

However, there's no need for severe disruptions to happen. By following the suggested steps, organizations can prepare for and execute a rollout that's smooth, deliberate, and efficient.

Step 1

Assess the organization's current security infrastructure

Before implementing MFA, it's crucial to understand and document existing authentication methods, systems currently in place, and the organization's data flow.

Identify current authentication methods in use
Authentication methods could be a simple username and password, security questions, or even an existing two-factor authentication system.

Analyze existing systems and how data flows between them
This analysis includes understanding the software, hardware, and network infrastructure. It's important to understand how authentication requests are currently handled and where potential vulnerabilities might exist.

Identify systems and data that need to be protected
Relevant systems can include customer databases, transaction systems, and internal communication systems.

Evaluate current security measures
Such measures could include firewalls, intrusion detection systems, and encryption protocols. Understand their effectiveness and where they might be lacking.

Conduct a risk assessment to identify potential threats and vulnerabilities
The risk assessment should consider both internal and external threats as well as the likelihood of a threat and the potential impact it could have.

Review any compliance requirements related to authentication and security
This review could include regulations like the General Data Protection Regulation, the Payment Card Industry Data Security Standard (PCI DSS), or specific regulations in the financial services sector like the *Bank Secrecy Act* or the *Sarbanes-Oxley Act* (SOX).

Step 2

Define the requirements for MFA

With current infrastructure assessed in detail, the organization can then define and document requirements for MFA. This process includes identifying the systems and data that need to be protected, the different types of users (such as employees and customers), and the level of security required. To define requirements, organizations should:

- **Identify the different user groups that will be using the MFA system**
  Examples of user groups include employees, customers, and vendors. Each user group might have different needs and requirements, so it's important to consider them separately.
- **Define the authentication requirements for each user group**
  Such requirements could include the types of authentication factors to be used (knowledge, possession, inherence), the level of security required, and any specific requirements for each user group.
- **Determine the system requirements for the MFA solution**
  The organization should identify existing systems that the MFA solution needs to integrate with as well as any additional requirements, such as scalability and performance.
- **Consider user experience requirements**
  An effective MFA solution should be simple to use and easy for users to integrate into their workflows. When evaluating the user experience, the organization should consider factors such as the time it takes to authenticate, the complexity of the authentication process, and the overall ease of use of the MFA solution.
- **Plan for future needs when defining the requirements for the MFA solution**
  Organizations evolve, and so do their MFA needs. Any organization's MFA solution should be scalable and flexible enough to accommodate future growth and changes in requirements.

Step 3

Choose an MFA solution

Many MFA solutions are available in the market – and choosing one can seem overwhelming. However, the requirements defined in step 2 can help organizations make the selection process more manageable. The most important points of differentiation to consider when choosing an MFA solution include ease of use, level of security provided, cost, and compatibility with existing systems.

In addition to evaluating options against requirements, participants involved in the selection process should ask the following questions when considering any potential solution:

Have we performed enough research into available solutions?

Thorough research doesn't require an evaluation of every option on the market. To narrow options, organizations can look for solutions that are widely used and have good reviews. They also can consider both stand-alone MFA solutions and those that are part of a larger security suite.

What is the vendor's reputation, and what level of support do they provide?

Organizations should identify vendors with strong track records in terms of security, reliability, and customer support. They also should consider the level of implementation support provided by the vendor, including technical support, training, and documentation.

How do the benefits of the solution compare to the costs?

The upfront costs and ongoing costs are important to take into account. When analyzing the benefits, organizations should include the enhanced security and any potential cost savings from preventing security breaches.

Can we test the solution before we decide?

Sufficient testing might involve setting up a trial or demo and piloting the MFA solution with a small group of users. This testing can provide a better understanding of how the MFA solution works and how it will fit into an existing infrastructure.

Once the organization has settled on a solution that best meets requirements and provides the best value for money, it's essential to document the decision and the reasons for choosing the MFA solution. This documentation can prove valuable for future reference and for communicating the decision to stakeholders.

Step 4

Implement the solution

The actual implementation process for an MFA solution includes configuration, integration with existing systems, and testing and reviews to evaluate how the solution is working and how successful the implementation process was. Steps for implementation include:

1

Developing an implementation plan

The implementation plan should outline the steps to be taken, resources required, an overall timeline, and the roles and responsibilities of the team members. The plan should also include a contingency strategy in case unforeseen issues arise during the implementation.

2

Configuring the MFA solution according to specific requirements

Configuration includes setting up the authentication factors, integrating the MFA solution with existing systems, and adjusting any settings as necessary.

3

Testing the solution to verify it works as expected

This process should include testing the authentication process, the integration with the existing systems, and the performance of the MFA solution. Any issues identified during testing should be resolved before the MFA solution rolls out.

4

Training the IT team on how to manage and support the MFA solution

Even the most carefully planned and smoothly executed MFA rollout will involve troubleshooting and IT requests. The organization's IT team should be fully trained on how to troubleshoot common issues, monitor the MFA solution, and update the MFA solution.

5

Preparing for and executing the rollout of the MFA solution

A successful rollout must involve communicating the change to the users, preparing training materials for the users, and setting up a support system to help users during the rollout. Once the rollout is underway, the organization should monitor the process closely to identify and resolve any issues that arise.

Deploying MFA at scale isn't a straightforward or perfectly smooth process. Many organizations that roll out MFA encounter unexpected issues – which can translate to valuable lessons for future technology initiatives. To discover those lessons, organizations should perform a post-implementation review and gather feedback to identify successes, issues, and areas for improvement.

02 Post-rollout: Monitor and update the MFA solution

A successful MFA rollout is a major milestone, but it's also only the beginning of an MFA journey. Organizations, threats, and MFA solutions all evolve over time. To verify that the MFA solution is still serving its purpose and providing the necessary level of security, the organization should regularly seek answers to the following questions:

? Is our MFA solution performing as expected?

To answer this question, the organization might monitor metrics such as the number of authentication attempts, the number of successful and failed authentications, and response times.

? Do performance metrics indicate any issues or trends?

Identifying issues and trends is critical for determining an internal or external problem. For example, a high number of failed authentications could indicate a problem with the MFA solution or a potential security threat.

? Is our solution still providing the necessary level of security?

Since security is paramount, the organization should conduct regular security audits to verify that the MFA solution is still delivering the necessary level of security. A security audit could include checking for any vulnerabilities or breaches, testing the MFA solution, and reviewing the security policies and procedures.

What do users say about their experiences with the solution?

MFA will always add an extra step, but an MFA solution should create minimum friction and disruptions for users. To continually deliver a smooth experience, the organization should review user feedback and identify any issues or areas for improvement. This process could include conducting surveys, holding focus groups, or reviewing support tickets.

Is our MFA solution still up to date?

The process of keeping the solution current can involve software updates and adding new authentication factors or changing configuration settings as needed. Any updates should receive testing before implementation.

Do users have the training and support they need to navigate any updates?

Whenever significant updates to the MFA solution are implemented, the organization should train users on these updates. Measures could include providing training materials, conducting training sessions, and providing one-on-one support.

Have we documented any changes or updates to the MFA solution?

Whenever significant changes are made, teams should document the nature of the changes, the reasons behind them, and the impacts.

03 Technical considerations for successful MFA implementation

An MFA implementation and rollout involves a blend of human and technical factors. As important as strategy, communication, and training are, technical considerations are equally vital to success and require equal attention. Following are several of the technical factors that are most likely to make or break an MFA implementation.

Understanding authentication protocols

When implementing MFA, it's important to understand the underlying authentication protocols. These protocols define how the authentication process is carried out and how the different authentication factors are verified. The following table explains the most common protocols and their implications for an MFA implementation.

Protocol	How it works	How it affects MFA strategy
Security assertion markup language (SAML)	SAML is like a passport system between two parties, typically a user and a service. Users validate their identities once, which is like getting a passport stamped. Then, they can use that validation to access multiple services without needing to log in again.	When using SAML, users need to make sure their MFA solution can integrate with it. For instance, after the first successful login (and MFA verification), users should be able to access multiple services without needing to go through MFA again.
Open authorization (OAuth)	Compared to SAML, OAuth is more like a valet key for a car. OAuth gives another party limited access to the user's resources without giving that party full control. OAuth is often used for "Log in with Google, Facebook, Twitter" prompts in which users give a service permission to access some of their data.	Since OAuth is about granting access to resources rather than verifying identity, it might not directly impact MFA. However, organizations should verify that the initial login process (which should include MFA) is secure when OAuth is used.
OpenID connect	OpenID Connect is an extension of OAuth. It's like the valet key, but it also includes a proof of identity, such as a driver's license. OpenID Connect is often used when a service needs to access resources and verify who users are.	OpenID Connect includes identity verification, so it can work well with MFA. When users log in through OpenID Connect, organizations can include MFA as part of the login process. Once the users are authenticated and verified, they can use the services without needing to reverify their identities or go through MFA again.

Understanding these protocols can help an organization choose an MFA solution that is compatible with its existing systems and meets its security requirements.

Encryption and secure connections

When implementing MFA, it's crucial to confirm that all connections are secure and all data is encrypted. Points for evaluation should include the connection between the user's device and the MFA server, the connection between the MFA server and the authentication server, and any connections to third-party services.

For secure connections, users should rely on protocols like HTTPS and secure virtual private networks. For data encryption, users should employ strong encryption algorithms and keep all encryption keys secure.

Database security

The MFA solution generally involves storing sensitive data, such as user credentials and authentication tokens, that must be kept secure. Steps that can help secure data include:

- **Encrypting the data**
- **Using secure database systems**
- **Regularly updating and patching the database systems**
- **Monitoring the database systems for any unauthorized access or suspicious activity**

Scalability and performance

The MFA solution should be able to scale and handle many users and authentication requests. Scalability considerations include the capacity to handle peak loads and the ability to scale up or down as the number of users or authentication requests changes.

In terms of performance, the authentication process should feel quick and seamless for users, with no significant delays or disruptions to their workflows.

Integration with existing systems

The MFA solution needs to integrate smoothly and seamlessly with the organization's existing systems, including user management systems, network infrastructure, security systems, and any other relevant systems. Achieving this smooth integration might require:

Application programming interfaces that allow applications to communicate

Middleware that helps isolated or separate systems interact

Custom integration solutions to bring together highly disparate systems

Compliance with regulations

In the financial services sector, compliance with all relevant regulations is a nonnegotiable requirement for any MFA solution and implementation. Notable regulations to consider during an MFA rollout include:

- **The *Gramm-Leach-Bliley Act***
  that governs the protection of consumer financial information

- **PCI DSS**
  for cardholder data

- **SOX**
  for fraud prevention in corporate information recordkeeping

Compliance efforts might involve selecting specific technologies or processes, conducting regular audits, or obtaining certain certifications. For example, under PCI DSS, multifactor authentication is required for all access that involves cardholder data and doesn't involve a direct, physical connection to a system component (also known as nonconsole access).

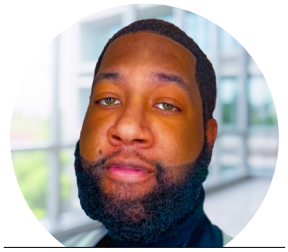
An MFA rollout is a complicated process with lots of potential pitfalls. **But Crowe specialists are here to guide you.**

Implementing multifactor authentication represents a crucial step toward enhancing security and protecting against unauthorized account access. While the process comes with its own set of challenges, the benefits are well worth it. With careful planning, the right MFA solution, and adequate user training, financial services organizations can significantly enhance their security and position themselves for long-term regulatory compliance.

Achieving a successful MFA rollout can be much easier if you're guided by a team of financial services specialists with deep knowledge and expertise in banking technology, cybersecurity, regulatory compliance, and digital transformation. When you need help, call us – we'll be there with tailored, practical solutions that match your needs, goals, regulatory requirements, and resources.

Explore cybersecurity services

David R. McKnight
Principal
Financial Services Consulting
+1 630 575 4399
dave.mcknight@crowe.com



Timothy Tipton
Financial Services Consulting
+1 202 552 8093
timothy.tipton@crowe.com

Sign up to receive the latest cybersecurity insights on identifying threats, managing risk, and strengthening your organization's security posture.

Explore Cybersecurity Watch

Smart decisions. Lasting value.™

CFS2409-002B