Sponsored content | White paper

Mainframe security: What financial services CIOs need to know about intensifying regulations

New and updated regulations such as DORA are placing pressure on financial services organizations to avoid significant penalties. They should start by rethinking mainframe security.

CIO

Sponsored by Rocket® software

Well-supported by highly skilled technicians, mainframes show no signs of disappearing. They remain the backbone of critical operations for financial services organizations.

Yet, new and updated regulations will require enterprises to take a closer look at their approach to mainframe security. The stakes are high. Non-compliance can result in penalties reaching millions of dollars.

Organizations that depend on terminal emulation and green-screen access for mainframe systems have struggled to apply modern security measures to them. Also, some organizations may not realize how these regulations apply to their mainframes because they're often seen and managed as a separate silo.

However, it's critical to recognize that mainframes are not exempt. Three major regulatory frameworks are reshaping mainframe security requirements this year:

- **Digital Operational Resilience Act (DORA):** Effective since January 17, 2025, DORA applies to organizations within the EU, as well as any enterprise conducting business there, with a particular focus on financial institutions. Its comprehensive approach to ensuring operational resilience includes specific provisions for systems like mainframes, requiring strong authentication such as multi-factor authentication (MFA).
- **Payment Card Industry Data Security Standard (PCI DSS):** Originally introduced in December 2004, PCI DSS underwent a significant update when version 4.0 took effect on March 31, 2025. This standard, developed by the payment card industry, focuses specifically on securing credit card and payment transaction data, much of which resides in mainframe systems.
- **New York State Department of Financial Services Cybersecurity Regulation:** The NYDFS 23 NYCRR Part 500 is partially in effect, with final requirements becoming mandatory on Nov. 1, 2025. It introduces stringent requirements across three critical domains: cybersecurity governance, encryption of non-public information, and incident response capabilities.

Specific considerations for DORA and PCI DSS

Despite their different origins and scopes, DORA and PCI DSS share common requirements that pertain directly to mainframe security, including:

- **Risk management:** Organizations must establish formal risk management frameworks, including designated managers and documented analysis plans.
- **Information security:** Strict guidelines govern how information can be shared both internally and externally.
- **Vulnerability management:** Mandates include continuous discovery and remediation of vulnerabilities, particularly those enabling privilege escalation.
- **Access control:** They require robust governance of authentication and authorization processes.
- **Data protection:** These regulations require the implementation of comprehensive strategies for data security and recovery.
- **Third-party supplier management:** Security requirements for external vendors and suppliers must be enforced,

which is particularly important for mainframes because they often employ open-source components.

- **Enhanced testing and reporting:** Rigorous threat testing and compliance reporting are now standard requirements.

That said, PCI DSS 4.0 introduces new changes. For example, organizations now have more flexibility to implement different security controls using customized, risk-based approaches.

Financial services institutions should also note the introduction of enhanced validation methods for testing security controls. Version 4.0 provides more guidance on how to validate PCI DSS requirements effectively.

There is also now a stronger emphasis on the necessity for ongoing monitoring and testing of security controls to ensure they are effective, as well as requirements around MFA to enhance security.

NYDFS 23 NYCRR Part 500: A closer look

The New York regulation deserves special attention. Chief information security officers must now implement cybersecurity governance, which entails the creation of specific plans for addressing material inadequacies in their written reports to senior governing bodies. In turn, these bodies are explicitly tasked with overseeing cybersecurity risk management strategies.

NYDFS also mandates written policies for industry-standard encryption of non-public personal information (NPI). For example, organizations can no longer use alternative compensating controls for encrypting NPI in transit over external networks, which has been a common practice in mainframe environments.

In addition, incident response and business continuity management requirements have been expanded. Incident response plans must now be updated and tested annually at a minimum, and all relevant employees must receive training on them. Organizations must also conduct testing exercises involving critical staff.

Small businesses face new requirements as well, including implementation of MFA for remote access to information systems, third-party applications containing NPI, and privileged information. Annual cybersecurity training should include social engineering and artificial intelligence (AI)-enhanced attack techniques.

The scale of the challenge

The security landscape is evolving rapidly. Bad actors are increasingly leveraging AI to deploy sophisticated attacks at scale, while regulatory requirements grow more numerous and complex with each update.

Organizations need a scalable risk management framework to meet these challenges. For mainframe environments, IT leaders need to examine how users are

accessing applications on mainframes and other host systems. They also need to know who is using the green screen and the assets to which they have access. Moreover, IT must be able to enforce policies governing permissions; blanket mainframe access will not be compliant.

In addition, homegrown security solutions often require substantial manual work to update and maintain. Manually attempting to find vulnerabilities in third-party code is cumbersome, inefficient, and error prone.

Strategic approaches to mainframe compliance

Financial services institutions hold and process incredible volumes of sensitive data on their mainframes. The stats may surprise even those who regularly work with mainframes. For example:

- **30 billion transactions are processed daily by IBM Z mainframes, including 90% of all airline transactions and 87% of all credit card transactions.**

With so much sensitive, critical data passing through these systems, organizations must rethink their approach to security. Mainframes are critical infrastructure deserving of the same robust protections implemented elsewhere in the enterprise.

The first step should be to identify where security policies are slowing or hampering business operations because they restrict data sharing. By implementing pervasive encryption across all systems, including mainframes, organizations can enable secure access to data while removing barriers to collaboration.

Authentication is another area on which to focus. In many mainframe environments, internal users have privileges that may be broader than necessary for their jobs. External users with privileged access can create significant vulnerabilities in mainframe environments.

Implementing MFA and enforcing least-privilege access policies can substantially mitigate these risks. In the long term, financial services institutions should adopt a zero-trust architecture that requires authentication at every point touching the mainframe.

IT teams can also reduce the risk of a successful attack or intrusion with a comprehensive vulnerability management program specifically designed for mainframe environments. Risk-based vulnerability management approaches give organizations a better understanding of their threat landscape and effectively prioritize mitigation efforts.

Modern mainframe security

Of course, organizations would struggle to tackle these efforts at the same time. After identifying the most critical assets to protect, create a top-down approach to resilience planning, starting with executive engagement, to determine organizational priorities.

CIOs, CSOs, and CISOs should work to break down departmental silos by facilitating collaboration with senior leadership. Seek to direct resources toward addressing the security and compliance concerns of the most important business functions.

Another consideration: Address response and recovery. DORA specifically requires systems to have a maximum of two hours downtime by design. Organizations must thoroughly document disaster recovery plans, clearly

outlining procedures, roles, responsibilities, and recovery strategies in easily accessible formats. The regulation also requires implementing surgical data recovery at the dataset and file level, along with automating disaster recovery life cycle phases.

How Rocket Software can help

Rocket Software has deep experience in modernizing and securing mainframe environments. Its security-first terminal emulation software, Rocket® Secure Host Access, fortifies green-screen interfaces with modern security controls. Solutions like this enable compliance with DORA, PCI DSS, and 23 NYCRR Part 500 by extending enterprise identity and access management best practices like MFA to the green screen, while also securing data with current encryption methods. Additionally, Secure Host Access enables single sign-on and automated sign on to the mainframe and other host systems, making user access easier and more secure.

The time to act is now; with final compliance deadlines approaching and significant penalties for non-compliance, mainframe security deserves a prominent place on every IT leader's strategic agenda.

Speak with **a Rocket Software expert, who can help guide your organization through the regulatory landscape and ensure your mainframe systems are ready for whatever comes next.**