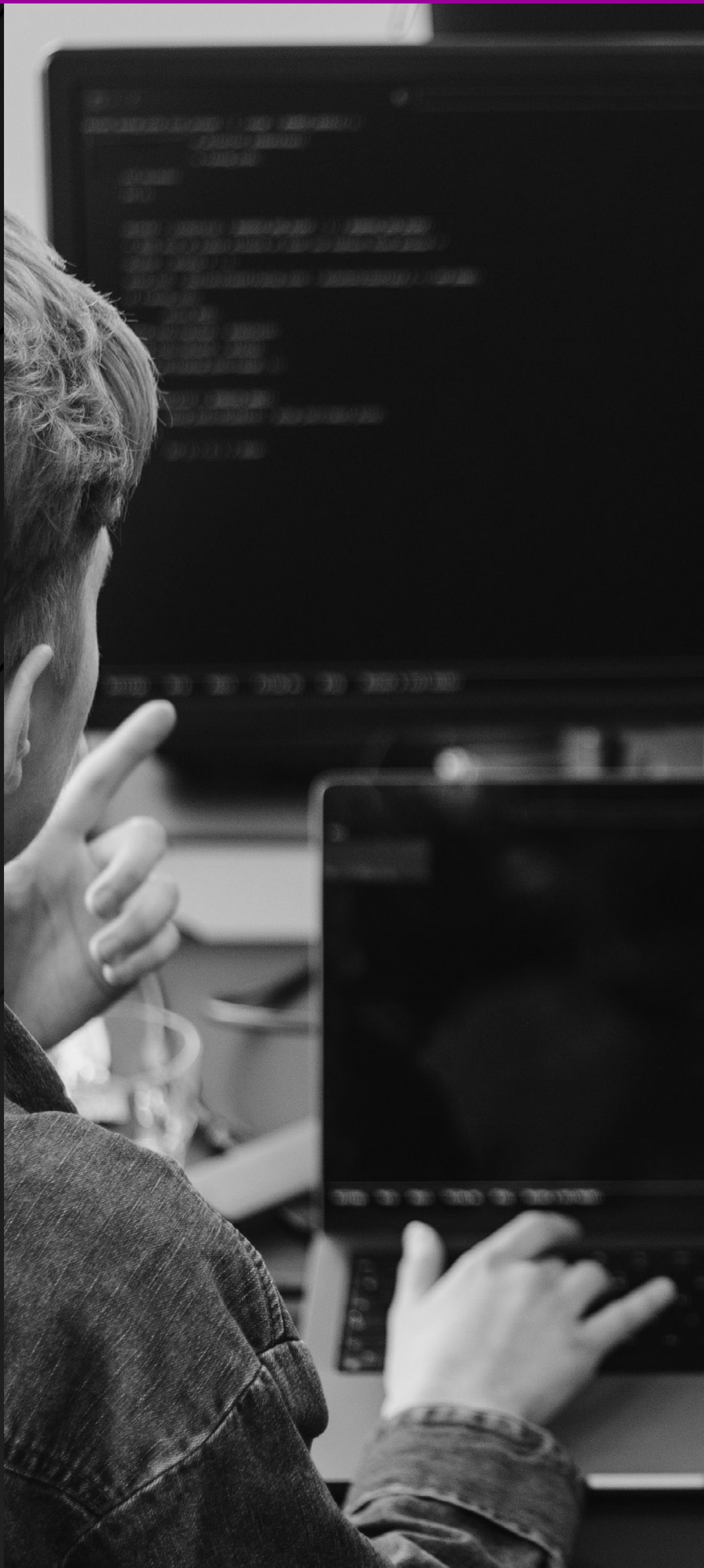
Rocket® software

Mastering Mainframe Risk Management: Your Starter Guide to Navigating Regulatory Changes

™



Contents

Introduction

Mainframes often fly under the radar when it comes to cybersecurity and risk management. Yet, they remain crucial to many organizations' IT infrastructure. Alarmingly, 91% of mainframe organizations have experienced a data breach or compromise within the last five years. Modern cybercriminals are advanced, sometimes financially backed, and even leveraging AI. This makes it imperative for businesses, especially in the financial sector, to address all mainframe vulnerabilities. Failing to do so could result in massive financial losses and regulatory penalties.

91%

of mainframe organizations have experienced a data breach or compromise within the last five years.

The importance of regulations

With new regulations such as DORA, PCI 4.0, and NIST continually updating requirements, financial and banking organizations need a comprehensive approach to their security or risk hefty penalties. These regulations guide global security expectations and compel organizations to advance their security measures to meet constantly evolving standards.

Key regulations guiding mainframe security

Digital Operational Resilience Act (DORA)

The Digital Operational Resilience Act (DORA) mandates financial services companies to upgrade, evaluate, and implement innovative systems and protocols to safeguard their data. Key requirements include routine risk assessments, regular vulnerability management on the mainframe, and ensuring rapid data recovery within a two-hour window.

PCI DSS 4.0

PCI DSS 4.0 emphasizes the need for comprehensive security measures to protect payment card data. This includes regular vulnerability assessments, robust authentication mechanisms, and stringent data privacy policies.

NIST Guidelines

The NIST guidelines provide a framework for improving the security and resilience of critical infrastructure. They emphasize the importance of continuous monitoring, vulnerability management, and incident response planning.

GDPR

GDPR empowers consumers by giving them greater control over how companies use their personal data. By standardizing data protection rules across the EU, it creates a clearer and simpler legal framework for businesses.

Key pillars of a mainframe risk management strategy

To build a robust risk management program for your mainframe, focus on four key pillars:

01

Implement a scalable mainframe vulnerability management program

A comprehensive vulnerability management program should cover both code-based and configuration-based vulnerabilities. Many regulations mandate that organizations address both types to ensure robust cybersecurity measures, and not implementing both leaves a gaping hole in cyber defenses.

Vulnerability scanning

Frequent vulnerability scanning is crucial. Multiple scans per year help identify deviations from policy and IBM®'s Statement of integrity. This proactive approach minimizes potential entry points for hackers.

Compliance assessment

Compliance checks must also extend to user access. An organization must periodically review user access on the mainframe and verify if it aligns with the company's security policies. Excessive access can lead to significant security risks.

> We never even thought we could have vulnerabilities on the mainframe, but once we began automated scanning, we found the volume and the severity to be much greater than anticipated."
>
> **- CISO**

02

Conduct penetration testing

Penetration testing goes beyond vulnerability scanning by simulating real-world hacking attempts. This proactive measure helps identify weaknesses that could be exploited.

Real-world simulation.

Penetration testers take on the role of hackers, trying to breach your mainframe. This process helps you understand potential vulnerabilities.

Regular testing

To adhere to regulations, penetration testing should be conducted several times a year. This ensures that your cybersecurity measures are up-to-date and resilient against evolving threats.

03

Address open source vulnerabilities

Open source can introduce vulnerabilities if not properly managed. Ensuring that all open-source software is fully supported and regularly updated is critical.

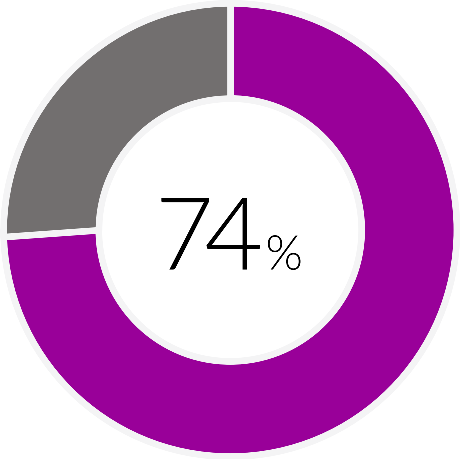
Supported open source

Using supported open-source software ensures that vulnerabilities are quickly addressed in line with the NIST national vulnerability database. Organizations must leverage software with access to the most recent versions and fixes to CVEs. Unsupported open source may only receive updates a few times a year, leaving significant windows of opportunity for attackers.

> Getting our penetration testers up to speed on the mainframe seemed like a tall task at the beginning, but it was well worth the time and effort we put into this initiative. And, our company is much more secure for it."
>
> **- CISO, GLOBAL BANK**

Proactive management

With open-source services and support, organizations can confidently stay secure with rapid updates, ensuring peace of mind every step of the way. This proactive management minimizes the risk of exploitation.



"Up from 48% the previous year, 74% of the open-source codebases contained high-risk vulnerabilities!"

04

Ensure surgical data recovery

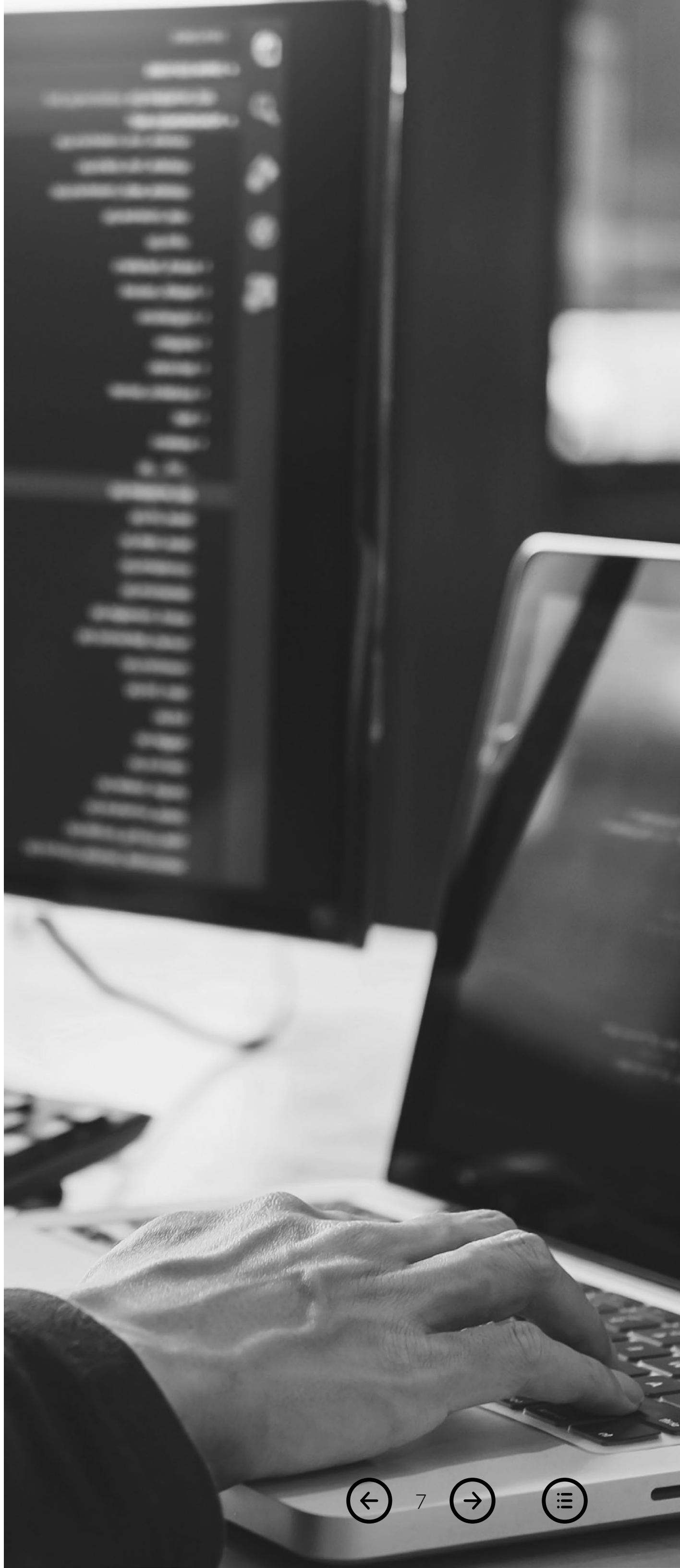
Data recovery is more than just restoring data; it's about precision and speed. Regulations like DORA now require organizations to recover data within a two-hour window by design.

Surgical recovery solutions

Using supported open-source software ensures that vulnerabilities are quickly addressed in line with the NIST national vulnerability database. Organizations must leverage software with access to the most recent versions and fixes to CVEs. Unsupported open source may only receive updates a few times a year, leaving significant windows of opportunity for attackers.

Regulatory compliance

Meeting regulatory requirements for data recovery ensures that your organization is resilient and can quickly bounce back from data breaches or other disruptions.



Conclusion

Mainframe security is not a one-time effort but an ongoing commitment. By understanding the vulnerabilities your mainframe faces and taking proactive steps to mitigate these risks, you can protect your enterprise from costly breaches and ensure compliance with industry regulations.

Ready to strengthen your mainframe security? Connect with our experts today. Together, we can create a robust security strategy tailored to your organization's needs.

Learn more

About Rocket Software

Rocket Software is the global technology leader in modernization and partner of choice that empowers the world's leading businesses on their modernization journeys, spanning core systems to the cloud. Trusted by over 12,500 customers and 750 partners, and with more than 3,000 global employees, Rocket Software enables customers to maximize their data, applications, and infrastructure to deliver critical services that power our modern world. Rocket Software is a privately held U.S. corporation headquartered in the Boston area with centers of excellence strategically located around the world. Rocket Software is portfolio company of Bain Capital Private Equity. Follow Rocket Software on LinkedIn and X (Formerly Twitter).

Rocket® software

Modernization. Without Disruption.™

Visit RocketSoftware.com ›