BROADCOM
MAINFRAME SOFTWARE

WHITE PAPER

Hybrid IT Compliance

The Definitive Guide

WHITE PAPER

Hybrid IT Compliance

The Definitive Guide

BROADCOM
MAINFRAME SOFTWARE

TABLE OF CONTENTS

Mainframes are a lot like banks. They hold some of the most valuable information in the world—which make them a lucrative target for everything from insider attacks to data theft. Mainframes today process approximately 90% of credit card transactions annually, and nearly 80% of all corporate data is secured and managed on the platform (The FutureScape of IT). The mainframe platform is clearly crucial to the hybrid IT ecosystem in helping deliver end-to-end customer experiences and drive digital transformation.

Overview

Mainframes are the most secure platform ever built; however, they are not impervious to cyber threats and regulatory mishaps. *Enterprises must use the right policies and security solutions to lean into the inherent security of the platform and comply with regulations.* Consider privileged users. The mainframe has built-in-security measures that can be bypassed by a stolen, lost, or shared credential—a scenario that unfortunately happens every day. In fact, compliance audits focus on ensuring that organizations have processes in place to protect against these types of threats.

The risks to mainframe data are growing by the day as are the regulations. Data privacy rules and regulations such as the General Data Protection Regulation are holding enterprises responsible for maintaining data integrity, and fines associated with non-compliance can reach as high as four percent of annual global revenue. Given that most enterprise organizations with a mainframe generate billions of dollars in annual revenue, it is easy to see how expensive noncompliance can become.

Enterprises today are faced with the same challenging questions: How do I pass my next compliance audit? How do I reduce the costs and efforts associated with passing an audit? What are the main compliance concerns for an enterprise processing large amounts of data? How do I resolve gaps and prepare the business for continuous compliance? Read on to find out.

A DATA-HUNGRY WORLD:

80%

OF ALL CORPORATE DATA STILL RUNS ON A MAINFRAME PLATFORM.

The Criticality of Mainframe Security

The mainframe runs everything from simple bank balance look-ups on mobile devices to billions of credit card transactions using advanced analytics. There is even more diversity in terms of types of workloads running on mainframe as organizations increasingly leverage hybrid IT to keep down IT costs. While this approach tends to reduce overhead, it also results in different types of workloads running on the mainframe—workloads that need to be both secured and audited to ensure compliance.

The assumption that gets made is that access to all those workloads is secure because the data is usually encrypted. However, current and former employees, contractors, and business associates that understand an organization's processes can wind up being complicit in everything from fraud to theft of intellectual property. It is the existence of these insider threats that makes limiting who can access what mainframe data a crucial element of any IT security strategy.

Unfortunately, not every organization has a robust program in place for managing privileged credentials. In a recent survey, 18% of respondents admitted they did not have a formal process in place to secure data against internal threats. (Create an Action Plan for Insider Threat)

Though important, mainframe security efforts should not be limited to insider threat mitigation. The mainframe has amassed data over the years. In a recent panel discussion on mainframe security and compliance, Rainer Barthel, Security Architect at Mainline, said, "Mainframe has the crown jewels, so it is the most important part to protect." Most companies do not know their data landscape. They cannot properly organize their mainframe data to adhere to security and auditing best practices, which increases the risk to business-critical data and systems.

MISSION-CRITICAL MAINFRAME DATA:

18%

OF ORGANIZATIONS DO NOT HAVE A FORMAL PROCESS IN PLACE TO SECURE DATA AGAINST INTERNAL THREATS.

Mapping Regulations to Your Business

Though compliance mandates may change over time, they never completely go away. In fact, each successive wave seems to bring with it more strident requirements. This rise in regulatory demand makes it increasingly difficult to stay on top of compliance mandates—and increasingly more important.

The following major compliance mandates are impacting mainframes:

- **General Data Protection Regulation (GDPR):** Drafted by the European Union, this compliance mandate is arguably the most comprehensive data privacy regulation to ever be enacted. Under GDPR, every company that maintains EU citizens' data must be able to perform the following tasks:
  - Protect personally identifiable information both at rest and motion
  - Delete personal data at the request of the individual
  - Move personal data at the request of the individual
  - Inform individuals of data breaches within 72 hours of an incident

A MODERN-DAY CONUNDRUM: THE RISE IN REGULATORY DEMAND MAKES IT INCREASINGLY DIFFICULT TO STAY ON TOP OF COMPLIANCE MANDATES.

- **Health Insurance Portability and Accountability Act (HIPAA):** The U.S. government established this regulation to address concerns about protecting healthcare data and maintaining privacy. HIPAA has the following two core components:
  - The Privacy Rule establishes national standards for the protection of health information.
  - The Security Standards for the Protection of Electronic Protected Health Information (the Security Rule) establishes a national set of security standards for protecting health information held or transferred in electronic form.
- **Payment Card Industry Data Security Standard (PCI DSS):** Developed mainly by providers of credit cards, PCI DSS mandates a standard approach to applying controls to how cardholder data is processed and stored.
- **Sarbanes-Oxley (SOX):** SOX addresses almost every aspect of financial reporting. It requires organizations to have a central oversight board tasked with registering auditors, defining the specific processes and procedures for compliance audits, inspecting and policing conduct and quality control, and enforcing compliance with specific mandates.
- **Federal Information Processing Standard 140-3 (FIPS 140-3):** Enacted by the U.S. government, FIPS 140-3 imposes mechanisms and controls for document processing, encryption algorithms and other elements of IT on both non-military government agencies, government contractors, and vendors who work with those agencies.
- **Security Technical Implementation Guides (STIGs):** STIGs are written by the Defense Information Systems Agency, which is a part of the U.S. Department of Defense (DoD). STIGs are a collection of technical guidelines covering multiple platforms—including mainframe, and they are designed to better secure systems and software from cyber attack. The guidelines are the configuration standards for the DoD, but they are often applied during compliance assessments in the civilian sector.

These requirements represent the tip of the potential compliance iceberg. Almost every country around the world has enacted some variation of these regulations with respect to data security and processing. In most cases, organizations that have mainframes are struggling to comply with dozens of compliance mandates at a time.

The Fundamentals of Any Compliance Audit

Time-consuming processes in compliance can sap your team's energy and budget. The fundamental goal of any IT organization is not only to pass a compliance audit, but to reduce the amount of time and resources required to maintain compliance. *The fact is, true compliance should foster business growth not disruption.*

THE FUNDAMENTAL GOAL OF ANY IT ORGANIZATION IS NOT ONLY TO PASS A COMPLIANCE AUDIT, BUT TO REDUCE THE AMOUNT OF TIME AND RESOURCES REQUIRED TO MAINTAIN COMPLIANCE.

Understanding the job of a compliance auditor is a key step towards achieving that goal. To start, a typical compliance audit involves the following steps:

- Achieving an understanding of the organization's business processes and relevant compliance regulations by reviewing relevant documentation and interviewing personnel
- Obtaining an understanding of how internal controls work, and then testing the effectiveness of those controls
- Evaluating the results and assessing the need for other controls and procedures
- Reviewing training dates and materials to ensure that the staff is properly educated on compliance policies
- Determining risks to the business based on potential issues of noncompliance

Each auditor is going to approach each of these tasks slightly differently, but the more an organization aims to understand the auditor's objectives, the better prepared that organization will be.

Best Practices on How to Achieve and Maintain Compliance

Organizations need to make sure they adhere to best practices for compliance from data security to governance to establish an effective compliance program. Those best practices should include a set of consistent policies and procedures inclusive of automation and operational intelligence. Best practices required to drive compliance broadly fall into three categories.

IT IS NOT POSSIBLE TO ACCURATELY ASSESS YOUR RISK POSTURE WITHOUT KNOWING WHERE YOUR DATA IS LOCATED—AND WHETHER IT IS BEING PROTECTED.

Data Discovery and Classification

The first step in achieving compliance is knowing where all your sensitive and regulated data resides, and you are able to easily show this capability to an auditor. It is not possible to accurately assess your risk posture without knowing where your data is located—and whether it is being protected. Once your data is located, business decisions can be made to appropriately secure, encrypt, archive, or delete that data.

Complex and toxic data combinations can affect your ability to identify sensitive and regulated data on the mainframe. Things get even more complicated when organizations start to realize how much disparate and unstructured data exists on the mainframe. While structured data is more likely to contain personally identifiable information (PII), there are many reasons why PII might find its way into an unstructured file.

Solutions such as *Data Content Discovery* can scan the mainframe to identify the location of sensitive data and classify that data based on regulatory or business need. Comprehensive reporting of scan results provides auditable trails for proof of compliance. Such tools help to mitigate data exposure risk and protect business-critical information.

IT TEAMS MUST WORK CLOSELY WITH BUSINESS UNITS AND HUMAN RESOURCES TO UNDERSTAND WHO NEEDS ACCESS TO SPECIFIC CLASSES OF DATA AND WHEN.

Compliance Management

Security must be a cross-enterprise endeavor requiring a holistic view of your entire hybrid IT environment. This view includes the mainframe. Comprehensive compliance management is critical for simplifying the regulatory compliance process and streamlining audits—a key aspect of maintaining cross-enterprise compliance while keeping costs low.

To do this, enterprises must implement automated compliance management solutions, such as *Compliance Event Manager*. Automated compliance management solutions must monitor users, security settings and system files, alert to changes and suspicious activity, filter and forward events to SIEMs and other platforms, and inspect the source of incidents. Compliance Event Manager is unique in that it includes partitioned data set monitoring—generating alerts to changes in critical mainframe configuration files that would otherwise be undetectable. This capability is critical for preventing breaches stemming from insider threats.

Privileged Access Control

The mainframe houses large amounts of data that is critical to driving your business. Keeping track of rights and privileges associated with accessing that data can be a major challenge. End users and internal IT teams look for the fastest method to complete work. This mindset can lead to shared passwords and credentials, bypassing even the best-laid compliance plans. Roles are also subject to change within any organization. People get promoted or switch jobs in organizations all the time, so rights should never be granted in perpetuity. IT teams must work closely with business units and human resources to understand who needs access to specific classes of data and when.

THE RIGHT STRATEGY IS FUNDAMENTAL TO RAISING THE BAR ON DIGITAL TRUST—ENSURING A BETTER CUSTOMER EXPERIENCE AND PROTECTING BUSINESS-CRITICAL DATA.

Software solutions such as *Trusted Access Manager for Z* control and monitor all activity performed by privileged accounts by promoting and demoting existing user identities based on business need. This solution helps to eliminate the risk of privileged credential sharing and reduce your overall risk posture. The solution also generates audit and forensic data on all activity performed by identities in their privileged state to provide a comprehensive view designed to simplify auditing. Solutions like *Cleanup* can also help to remove obsolete, unused, redundant and excessive entitlements, identities, and access rights to further reduce risk.

Compliance is indispensable to the modern business. The right strategy is fundamental to raising the bar on digital trust—ensuring a better customer experience and protecting business-critical data. Incorporate industry best practices from data security to privileged access management to achieve and maintain continuous compliance.

Why Compliance is a Cross-Enterprise Endeavor

Regulatory compliance requires coordination across all data and all systems—making compliance a shared responsibility.

Typically, the requisite controls are defined by a dedicated risk organization that examines everything from sustainability to business continuity. It is then up to the security and IT departments to implement those controls. It is also not uncommon for the IT infrastructure to be subjected to an audit by an internal risk assessment team. This exercise prepares the enterprise for an external audit—identifying potential gaps before an auditor does.

2X

HIGHER-GROWTH COMPANIES VIEW RISK MANAGEMENT AS CRUCIAL.

In many cases, the budget for acquiring and implementing compliance processes resides within a centralized risk management organization. It is worth noting though that not every organization is as far down the path as others. In a recent survey, higher-growth companies were twice as likely to view risk management as crucial for growth than their lower-growth counterparts, and 50% of organizations were without a Chief Risk Officer (Reimagine Risk: Thrive in Your Evolving Ecosystem).

Ask the Expert: Learn How to Address Regulatory Concern on the Mainframe

Where Does the Mainframe Factor Into the Overall Security Strategy?

The Chief Information Security Officer is often focused on the distributed environment; however, cross-enterprise security is critical to securing mission-essential data and complying with the regulations. Most corporate data still resides on the mainframe—and most transactions run on the platform. The mainframe is the most secure platform, but it is not immune to regulatory mishaps and cyber threats. Enterprises must take advantage of advanced security solutions including privileged access management and multi-factor authentication to effectively secure the enterprise mobile-to-mainframe.

Are the Standard Security Procedures on the Mainframe Changing?

The standards are certainly changing. There were not many regulations 50 years ago. Policies and procedures for the mainframe must now adapt to regulatory requirements defining standards for data collection, storage, and protection. Enterprises for instance, are spending a lot more time identifying, classifying, and protecting key fields and key records of data. Reporting is critical too—being able to create an auditable trail.

50%

OF ORGANIZATIONS ARE WITHOUT A CHIEF RISK OFFICER.

What are the Fundamentals of a Compliance Audit?

The auditor typically starts by reviewing the organization's business strategies, various job roles and responsibilities, and current policies and procedures. The auditor will then outline the objectives across key areas and determine whether the organization has established controls defined by the regulations. The audit includes interviewing personnel to ensure that they understand and adhere to those controls. The compliance audit will also include an assessment of the devices and equipment, and a review of the organization's system of reporting. The final audit report will highlight failure areas in need of remediation and additional controls required to manage risk.

Have More Questions?

Request a conversation with an expert at mainframe.broadcom.com/contact.

ORGANIZATIONS THAT PROACTIVELY ADDRESS COMPLIANCE REGULATIONS ARE AMONG THE MOST TRUSTED IN THE WORLD.

The True Value of Compliance

The goal of compliance is twofold: build a stronger business, and reduce the risks of noncompliance. This goal requires a concerted effort across the entire organization mobile-to-mainframe. It takes the support of several teams to achieve and maintain compliance with the litany of regulatory mandates; however, organizations that proactively comply with these regulations are among the most trusted in the world. This trust almost always results in higher brand equity and greater customer retention—both of which drive business growth. Given both the tangible and intangible costs associated with failing to meet compliance mandates, it is fair to say compliance with the regulations is nothing short of priceless.

For more information, please visit mainframe.broadcom.com.

Learn how Broadcom can help with your next compliance audit.

Visit us today: broadcom.com/products/mainframe

BROADCOM
MAINFRAME SOFTWARE

About Broadcom Mainframe Software

Broadcom Mainframe Software empowers customers to amplify the value of their mainframe investments. Our commitment to partnership is grounded in delivering to customers greater success with the platform. It starts with embracing open technologies in ways that unite the mainframe and hybrid cloud environments. Our leading DevOps, AIOps, Security, Data Management, and Core Infrastructure software solutions and innovative value programs go beyond code to unlock the platform's full potential.

For more information, visit our website at: mainframe.broadcom.com

HIC-TDG-WP100 August 22, 2022