CPT Global presents

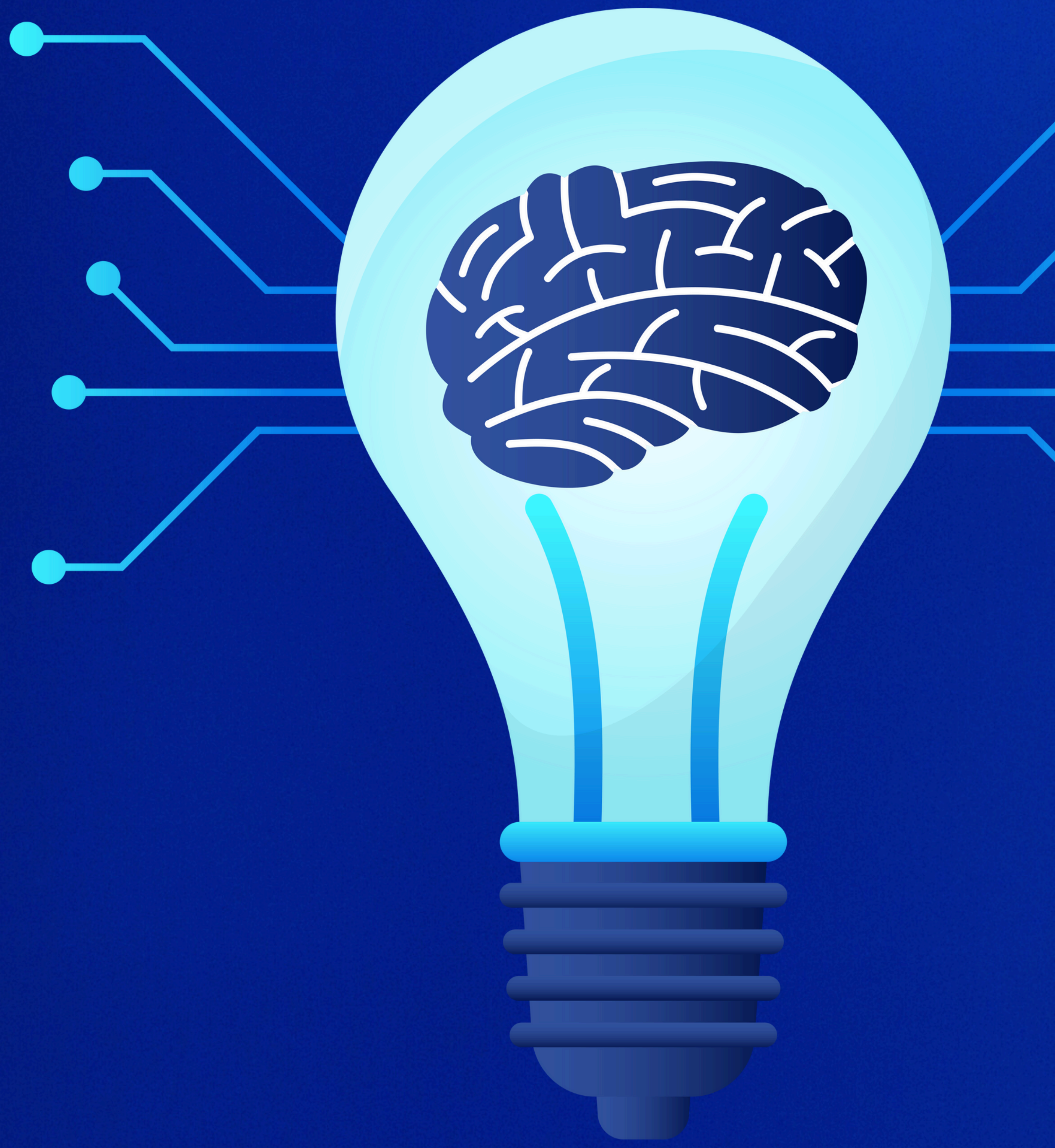
Invisible Compliance Traps

The Mainframe Security Gaps That Regulators Seek

Introduction

Mainframes have powered businesses for decades, but regulatory landscapes are shifting, and so are the risks. Too often, teams assume mainframes are "set and forget" platforms – reliable, yes, but immune to modern compliance pitfalls? Not at all.

In this whitepaper, we explore why overlooked vulnerabilities create compliance trouble – and how deeper insight, practical assessment, and targeted remediation can turn risk into resilience.



The Problem Beneath the Surface

When mainframe owners think about compliance, they often tick boxes: Is an External Security Manager (ESM) in place? Are system datasets controlled? Is there a password policy? Yet, it's not enough simply to have technical controls. How you implement, monitor, and refine them matters.

Recent updates to frameworks like DORA, PCI DSS, HIPAA, and GDPR highlight the need for continuous, proactive mainframe security.

Common Culprits include:

Weak or Outdated Configurations

Poorly configured environments, missed patch cycles, or outdated controls give attackers room to maneuver.

Improperly Secured System Datasets

Exposed datasets aren't rare – and regulators are taking notice.

Over-Permissioned User IDs

Accumulated user authorities and "toxic combinations" break the principle of least privilege.

Underutilized Security Features

Many organizations have an ESM - but only scratch the surface of what these tools offer.

How Compliance Failures Take Shape

A recent security assessment performed by CPT Global revealed significant vulnerabilities in a company's system, stemming from configuration weaknesses.

These factors led to exposed resources, unchecked admin privileges, and slow progress on essential patching. The assessment identified numerous vulnerabilities – gaps that were almost guaranteed to earn the business a negative audit and regulatory fallout.

These issues are not unique to one organization. When documentation fails to clearly show who has which rights or which datasets remain unprotected, proving compliance with regulations like HIPAA, PCI DSS, DORA, or GDPR becomes a significant challenge.

Issues Detected

Disconnected security responsibilities

Outsourcing services without managing overall security risk.

Poorly managed RACF database

Resulting from inadequate knowledge transfer.

Inherited privileges

New staff profiles created from existing user roles, leading to unnecessary privileges.

Turning Exposure into Action: CPT Global’s Approach

Solving invisible compliance traps is not about introducing more tools. It’s about maximizing the value of what you already own, optimizing processes, and enforcing governance. Here’s how CPT Global helps organizations close the loop.

Policy & Procedure Review

Action: Examine security documentation, process adherence, and alignment across controls.

Why? Unclear or outdated policies create gaps and are a red flag for regulators.

Access Controls & Privilege Audits

Action: Uncover over-permissioned accounts and insufficient segregation of duties.

Why? Provides a clean, prioritized map to align access with roles.

Configuration & Security Assessment

Action: Check protection of critical resources, logging, and full ESM feature implementation.

Why? Reveals technical debt and steps to meet regulatory standards.

Password & Authentication Practices

Action: Review password rotation, strength, and multi-factor authentication.

Why? Regulators increasingly mandate robust authentication, not "set and forget" policies.

Success Story

US Financial Services Company Gets Its House in Order

A leading US financial services company faced a critical challenge: their z/OS resources were wide open, features were turned off or ignored, and security ownership was split between in-house and outsourced teams. This resulted in a patchwork security posture.

Our Solution

When CPT Global conducted a remote security assessment, we discovered hundreds of vulnerabilities, including improperly secured datasets, insecure settings, and user IDs with excessive permissions accumulated over years of role shuffling.

Client Wins

To address these issues, our experts provided immediate, actionable guidance. We recommended creating a Mainframe Security Engineering role to bridge process and technical gaps, delivered focused training, and mapped out a practical and achievable three-year security roadmap.

With these steps in place, the client consolidated governance, closed urgent security gaps, and brought their environment back into regulatory alignment.

Investing in Security as a Business Priority

Security isn't a set-and-forget checkbox. It's woven into the way your business operates and competes. Skimping on security may offer short-term savings, but the true costs surface quickly and painfully.

SHORT-TERM COSTS

Regulatory Fines

Non-compliance with DORA, PCI DSS, HIPAA, or GDPR can trigger hefty penalties, sometimes running into the millions.

Operational Disruptions

Unpatched vulnerabilities or mismanaged user rights lead to downtime, lost productivity, and emergency remediation costs.

Audit Failures

Scrambling to satisfy auditors after the fact is more disruptive and expensive than maintaining a strong baseline day-to-day.

LONG-TERM CONSEQUENCES

Reputational Damage

Customers and partners lose trust in organizations that suffer breaches. Recovery can take years, if it's possible at all.

Legal Exposure

Data breaches may result in lawsuits, contractual breaches, or long-term regulatory oversight.

Innovation Bottlenecks

Insecure technology environments breed hesitancy to modernize, slowing transformation and increasing opportunity costs.

cpt

The Case for Proactive Investment

The ROI is practical and measurable. Security investments protect against catastrophic loss, enable confident compliance, and strengthen the business case for future-facing projects.

Aligning your security agenda with business goals turns risk management into a value driver, not just an overhead cost.

Treating security as a proactive, ongoing business priority returns more than peace of mind. It translates into:

✓ Managed Risks and Costs

Investing in assessment, governance, and efficient remediation keeps risks measured, and the cost of incidents down.

✓ Operational Resilience

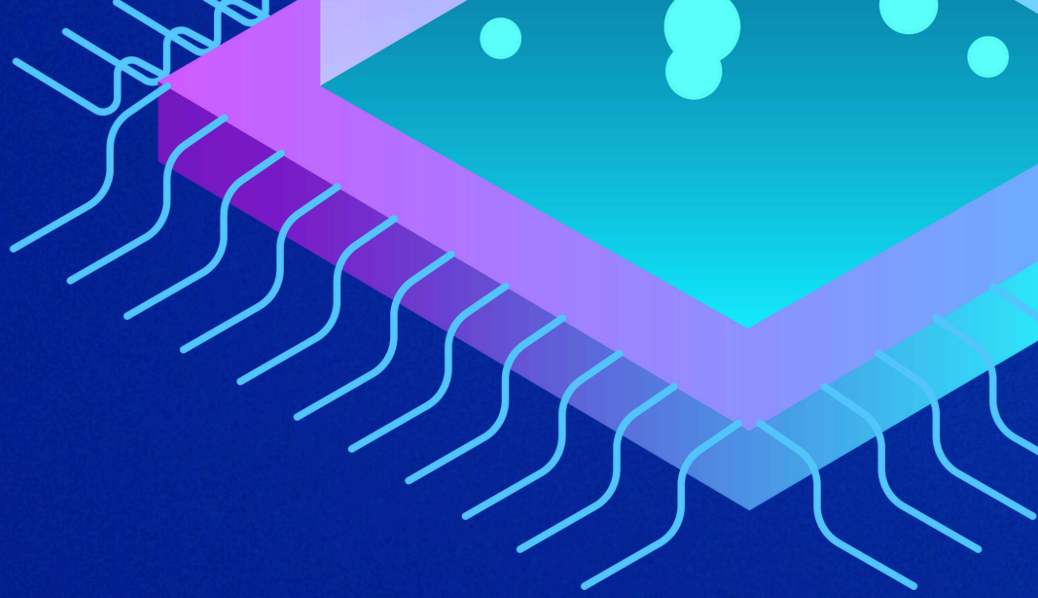
A secure mainframe environment keeps critical services running, no matter what's thrown at it.

✓ Growth Enablement

When your foundation is secure, transformation and innovation move faster – with less friction and lower risk to the business.

✓ Competitive Edge

Demonstrable security is a differentiator in regulated industries and builds trust with customers and regulators alike.



3 Examples of the Costs of Poor IT Security

Equifax Data Breach (2017) & Lingering Impact

Despite its age, this breach remains a prime example of mainframe-adjacent vulnerabilities.

Equifax failed to properly secure "mainframe-connected systems," allowing attackers to move laterally and access sensitive data. This highlights a failure to manage the security of systems adjacent to the mainframe, resulting in a breach that led to over $1.4 billion in settlements and remediation.

ICBC Ransomware Attack (2023)

A ransomware attack on ICBC significantly disrupted a $26 billion market. While the breach wasn't directly on the mainframe, ICBC failed to protect its interconnected operations.

The attack affected a major financial institution heavily reliant on mainframes and disrupted the US Treasury market, which shows that a security failure in one area can have a cascading impact on critical mainframe-dependent services.

Mainframe "Blind Spots" & Breach Costs (2025)

Industry reports, like IBM's 2024 Cost of a Data Breach Report, show financial sector breaches average $6.08 million.

Companies often fail to monitor privileged access, CICS transaction gaps, or insecure batch jobs. These overlooked areas contribute significantly to data exposure, fraud, and compliance failures because they enable attackers to exploit weaknesses that are not widely publicized or regularly checked.

Getting Ahead of Compliance Gaps

Regular, End-to-End Assessments

Don’t rely on routine audit checklists. Commit to annual deep-dives across system configs, user rights, and operational procedures.

Embrace Governance as a Living Process

Adapt procedures to environmental, team, and regulatory shifts. Regularly review access, password, and security policy adherence, not just for external audits.

Centralize & Clarify Security Responsibilities

Avoid the “someone else has this covered” syndrome by assigning clear mainframe security ownership.

Unlock Value in What You Have

Review your licensed mainframe tools. Implement current security features, logging, and monitoring. Utilize existing resources fully before investing in new platforms.

Remediate, Don’t Just Identify

Findings are only useful if you act. Build a remediation plan with specific deadlines and accountability.

Mainframe security is a continuous effort, as most risks stem from neglect or human error, not malice. By proactively assessing your systems and using existing capabilities, you can ensure compliance and boost your mainframe's business value.

Let’s Secure Your Mainframe

If you’re ready to identify the invisible compliance traps in your environment, CPT Global can help turn underutilized security controls and fragmented processes into a platform for secure, compliant, and future-ready operations.

CONTACT: info@cptglobal.com
VISIT: www.cptglobal.com
FOLLOW: https://www.linkedin.com/company/cpt-global