SAI360
RISK FROM EVERY ANGLE

Building a Security-First Culture: From Reactive Compliance to Proactive IT Risk Management

Table of Contents

The InfoSec Reality

Chief Information Security Officers (CISOs) have one of the most challenging roles in the enterprise. Their remit spans deep technical expertise, regulatory compliance, and strategic business alignment. While they remain accountable for safeguarding systems and data at a granular level, their influence increasingly extends to enterprise resilience, regulatory assurance, and reputational risk.

Information security is now a core governance priority, with regulations evolving to match the increasing sophistication of cyber threats. Frameworks like the Digital Operational Resilience Act (DORA) and the NIS2 Directive require enterprises to implement enterprise-wide cybersecurity and operational resilience measures. Meanwhile, the Cyber Resilience Act (CRA) introduces security obligations at the technology and product level. These regulations embed cyber resilience into law, driving tighter integration between information security, compliance, and business risk functions.

What was once a siloed function now demands a strategic voice. Organizations are elevating cybersecurity into the boardroom, recognizing its impact on enterprise risk and resilience. Today's boards and regulators expect more from CISOs than technical fixes—they want measurable outcomes, clear visibility into risk, and assurance that security controls are aligned with business and compliance priorities.

A mindset shift is at the heart of this evolution. IT risk isn't just a security function; it's an enterprise-wide compliance and strategic imperative. For CISOs, this means moving beyond reactive compliance toward proactive, integrated risk management—embedding security into the fabric of the business's operations.

This paper explores the challenges slowing progress, the drivers reshaping information security, and the integrated models forward-thinking organizations adopt to thrive in the new era of digital risk and opportunity.

Aligning Security, Compliance, and Business Risk

As regulatory expectations evolve, information security teams are under pressure to demonstrate control implementation and compliance outcomes. CISOs increasingly find themselves translating deeply technical measures into terms that resonate with governance, risk, compliance, and audit stakeholders.

This shift is driven, in part, by regulation. Frameworks like DORA, NIS2, the Cyber Resilience Act, and GDPR explicitly require traceability from governance policies to technical controls and demand proof that these controls are actively maintained and monitored. In the aftermath of a cybersecurity incident or data breach, regulatory investigation or enforcement action is now one of the biggest concerns for firms. In many cases, the regulator's first question is, Can you provide evidence of control effectiveness?

Regulatory Themes Impacting CISOs

To fully grasp the operational and strategic impact on CISOs, examining key regulatory themes and the new demands they place on information security functions is helpful.

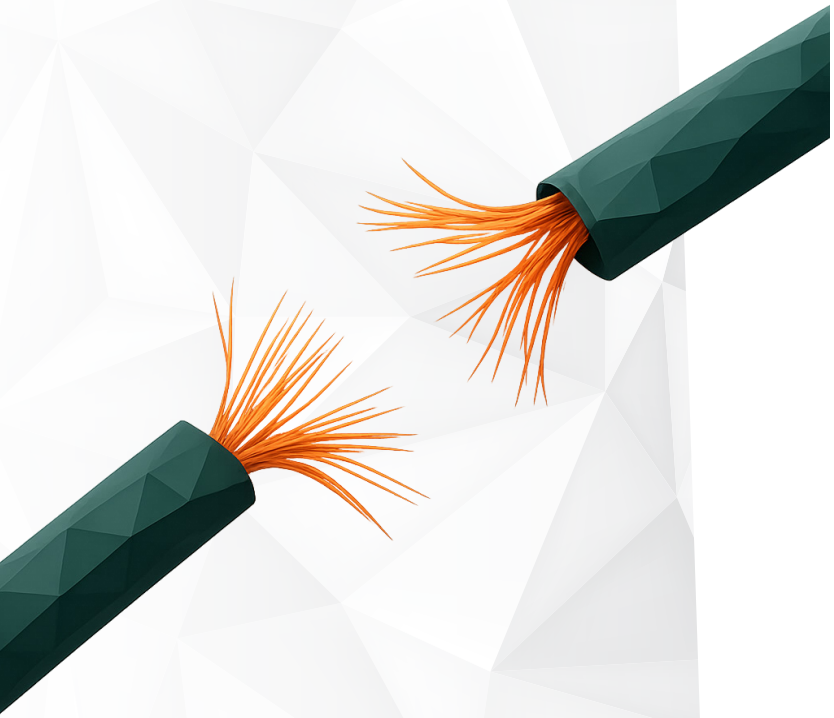
Regulatory investigation or enforcement action has become the leading concern for organizations in the aftermath of a cybersecurity incident or data breach, with 70% of cybersecurity professionals identifying it as their primary concern. Security efforts must align not only with compliance requirements but also with broader business objectives. Breaking down historical barriers between IT, security, risk, and compliance functions has become a structural necessity for organizations aiming to build resilience and maintain trust. But integration isn't just about shared tooling or dashboards. It requires fundamental organizational change:

- InfoSec must embed within enterprise risk frameworks, participating in governance and assurance alongside other risk functions.
- GRC teams must be able to interpret and act on security data, translating control telemetry into meaningful risk indicators.

Policies must map to controls in real-time, ensuring that what is on paper reflects what is implemented in the systems.

Regulatory Theme	Key Regulations	InfoSec Responsibilities	Why it Matters
Data Protection & Privacy	GDPR (EU General Data Protection Regulation) UK Data Protection Act 2018 (plus UK GDPR after Brexit) CCPA/CPRA – California Consumer Privacy Act and California Privacy Rights Act (United States – privacy rights and protections for California residents) APPI – Act on the Protection of Personal Information (Japan – national privacy law governing personal data use) PDPA – Personal Data Protection Act (Singapore – framework for personal data protection in the private sector) LGPD – Lei Geral de Proteção de Dados (Brazil – comprehensive data protection law modeled after the GDPR)	These laws primarily task CISOs with ensuring data confidentiality, integrity, and availability. Key responsibilities include: • Implementing technical and organizational measures to protect personal data • Breach detection and notification processes (often with strict timelines, e.g., 72 hours under GDPR) • Embedding data protection by design and by default (e.g., privacy engineering, secure development practices)	Privacy regulations transformed information security from a purely technical discipline into a legal and compliance-driven one. CISOs must now work closely with legal teams and data protection officers to translate privacy principles into system architecture, operational controls, and accountability frameworks.
Cybersecurity & Operational Resilience	DORA (Digital Operational Resilience Act – EU, financial sector) NIS2 Directive (EU critical entities) Cyber Resilience Act (CRA) (EU, product and software security) SEC Cybersecurity Rules (US, listed companies) FFIEC Cybersecurity Assessment Tool, NYDFS Part 500 (US, financial services) MAS Technology Risk Management (TRM) Guidelines (Singapore) HKMA Cybersecurity Fortification Initiative (CFI) (Hong Kong)	These frameworks establish technical and governance baseline expectations, including: • Incident detection, response, and recovery • Penetration testing and threat-led red teaming • ICT risk management and oversight of third-party service providers • Secure development lifecycle management and addressing software supply chain risks • Reporting and escalation of significant cybersecurity incidents within set timeframes	Cyber resilience regulations are formalizing and standardizing what was once best practice. InfoSec teams are now required to deliver repeatable, auditable, and measurable outcomes—often in coordination with risk, compliance, and audit functions. CISOs are becoming architects of digital trust and systemic resilience.

Regulatory Theme	Key Regulations	InfoSec Responsibilities	Why it Matters
Incident Reporting & Disclosure	GDPR Articles 33/34 (EU, personal data breach notification) DORA (EU, major ICT incident reporting within strict timelines) NIS2 Directive (EU, cybersecurity incident reporting within 24 hours) SEC Cybersecurity Disclosure Rules (2023) (US-listed companies, disclosure within four business days for material incidents) APRA CPS 234 and CPS 230 (Australia, 72-hour reporting requirement) NYDFS Cybersecurity Regulation	CISO-led teams must: • Detect and assess the impact of incidents rapidly • Document the incident timeline, root cause, and remediation actions • Coordinate regulatory and stakeholder disclosures with legal, compliance, communications, and executive leadership • Communicate proactively with regulators, affected stakeholders, and, where necessary, the public	Incident reporting regulations have driven a significant evolution in security operations' maturity. They have introduced regulatory urgency around forensic readiness, log retention, rapid incident assessment, and effective incident classification. InfoSec teams must now be as skilled at incident storytelling and regulatory communication as they are at threat containment and technical response.
Product & Software Security	Cyber Resilience Act (EU – cybersecurity requirements for products with digital elements) EU AI Act (high-risk AI systems, lifecycle security obligations) US Executive Order on Improving the Nation's Cybersecurity (including secure software development practices) FDA Cybersecurity Guidance (US – premarket and postmarket security for medical devices) IoT Cybersecurity Improvement Act (US – federal procurement standards for IoT devices)	For product-focused companies, CISOs and their teams are increasingly responsible for: • Ensuring secure-by-design principles across development • Managing vulnerabilities in embedded systems and software supply chains • Creating SBOMs (Software Bill of Materials) • Ongoing monitoring and patching of shipped products	Security is no longer just about protecting internal operations, but also about protecting the products and services that businesses deliver to their customers. CISOs must increasingly act as product risk specialists, collaborating closely with engineering, DevOps, and customer success teams to ensure security, resilience, and compliance with regulations across the entire product lifecycle.



Challenges Slowing Progress

Security ≠ Compliance

In many organizations, security and compliance aim to manage risk, but they approach it from different perspectives. Security teams focus on technical controls, such as firewalls, multifactor authentication (MFA), and vulnerability scanning. Compliance teams, on the other hand, concentrate on procedural and governance controls, including access reviews and policy attestations.

The result? A fragmented landscape where two sides struggle to align. Security engineers rely on purpose-built tools for real-time operations, such as incident response and patch management. In contrast, compliance teams often use GRC platforms or spreadsheets to track high-level control requirements. These systems don't always integrate, making translating what's happening on the ground into actionable, auditable evidence difficult.

This lack of interoperability means what is done in practice is not always captured in compliance documentation. A security team may be diligently patching systems, but it may go unreported unless that activity is logged in a format recognized by the compliance function. Conversely, compliance might indicate that encryption is enabled across the enterprise, but it lacks the details to show whether the implementation is robust.

Such disconnects create structural weaknesses in an organization's risk posture. Compliance efforts can overstate security maturity, giving stakeholders and auditors a false sense of assurance. At the same time, security teams may under-report their effectiveness, simply because they lack a mechanism to present operational data as formal compliance evidence.

Treating compliance and security as separate exercises leads to duplicated effort, misaligned priorities, and incomplete oversight. For many CISOs and IT risk leaders, the real challenge lies in bridging the gap—finding ways to integrate disparate tools and data sources so that compliance reflects actual security performance, and security efforts are appropriately evidenced and auditable in real time.

Reactive Compliance

Too many information security programs remain reactive, geared toward passing audits, meeting new regulatory deadlines, or fixing gaps only after incidents occur. While these triggers are essential, relying on them as the primary drivers of compliance leads to a cycle of short-term fixes and long-term risk accumulation.

Annual audits, for example, often prompt intense but temporary bursts of compliance activity. Policies are reviewed, access rights are checked, and documentation is updated—all in preparation for the auditor's arrival. Once the audit is complete, attention wanes until the cycle repeats. This audit-driven rhythm creates windows of vulnerability where control failures can go unnoticed for months.

Similarly, regulatory deadlines can catalyze action but must also prompt sustained and embedded change. Organizations often scramble to meet minimum requirements, treating compliance as a one-off project rather than an ongoing discipline.

Breaking this cycle requires shifting to a proactive security compliance model that embeds compliance into IT operations, emphasizes prevention and continuous visibility, and utilizes automation to monitor control effectiveness in real-time. This approach ensures that compliance is not just an annual exercise but an integral, always-on component of operational resilience.

Security Versus Business Agility

Information security has long walked a tightrope between protection and progress. Its role as a safeguard can be overshadowed by perception as an obstacle to speed, innovation, and user autonomy.

Rigid security controls, while essential, can feel burdensome when applied without nuance. Mandating multi-factor authentication, restricting administrative privileges, or enforcing strict change controls are sound practices from a risk perspective, but they may frustrate users or slow delivery timelines.

The root of the issue often lies in one-size-fits-all compliance. Policies written for high-risk systems are applied universally, creating unnecessary friction in low-risk scenarios while offering little additional protection. Yet granting too many exceptions in the name of speed can quickly erode security baselines, introducing inconsistency and exposure.

The modern security challenge is not simply to enforce controls, but to embed them into agile business processes in a way that supports, rather than impedes, momentum. CISOs and InfoSec leaders must update their frameworks, training, and expectations to reflect this new reality. When security becomes embedded in the business's rhythms and incentives, it stops being a roadblock and becomes a catalyst, empowering the organization to innovate quickly, confidently, and securely.

The Future: Aligning Security, Compliance, and Business Objectives

The path forward for information security lies in integration. Successful InfoSec programs are built on alignment across three critical domains: security, compliance, and business objectives. While distinct, these domains must work in concert to create a resilient, agile enterprise:

- **Security** delivers the technical implementation of safeguards and controls.
- **Compliance** provides the regulatory and policy frameworks that guide governance.
- **Business objectives** define the context—balancing innovation, risk appetite, and operational efficiency.

Where these elements converge is where the modern InfoSec function takes shape: risk-aligned, strategically embedded, and operationally effective. This evolution is enabled by connected GRC platforms that unify oversight, automate evidence collection, and unite stakeholders across functions. It is powered by shared data, real-time dashboards, and continuous monitoring, transforming compliance from a periodic event into a living, dynamic practice.

Adopting this integrated model delivers measurable value, including real-time visibility into compliance status, proactive risk mitigation, and scalable assurance that can adapt to business changes. Organizations no longer have to choose between security and agility. By embedding security into the enterprise's fabric, they can move fast, stay compliant, and innovate with confidence, building resilience as a competitive advantage.

SAI360 is giving companies a new perspective on risk management. By integrating ethics, governance, risk, and compliance within a single platform, SAI360 helps companies broader their risk horizon so they can manage risk from every angle.
Visit sai360.com to learn more.

000000 0624