SAI360
RISK FROM EVERY ANGLE

The Illusion of Control: Why Most IT Risk Frameworks Don’t Deliver

Table of Contents

Introduction

Fewer than half of CISOs are involved in company-wide strategic planning, a gap rooted in legacy organizational structures in which cybersecurity has been confined to the IT domain. This legacy mindset is now a liability, with most firms underprepared for modern technology risks: just 2% of executives say their company has implemented cyber resilience across all critical areas, including cloud platforms, generative AI, and third-party providers.[1]

IT resilience must be a board-level priority, with all stakeholders aligned to ensure security measures support enterprise goals, enable agility, and build genuine resilience. This connection and awareness is essential because, without it, firms risk fragmented oversight, misaligned priorities, and blind spots that expose them to both regulatory penalties and operational disruptions.

Turning conceptual alignment into operational execution requires a consolidated risk management architecture that delivers real-time visibility, fosters shared accountability, and provides control at scale. Making this a day-to-day reality is still an uphill battle.

In this paper, we examine how InfoSec leaders can break down silos and establish frameworks that enable sustainable, proactive IT risk management.

1. https://www.pwc.com/ca/en/services/consulting/cybersecurity-privacy.html

Building a Practical IT Risk Management Framework

The regulatory landscape governing IT risk management is complex and inconsistent. In some jurisdictions, notably the UK and Europe, regulators have imposed stringent requirements through initiatives such as the UK's Operational Resilience rules, the EU's Digital Operational Resilience Act (DORA), and the revised Network and Information Security Directive (NIS2). Elsewhere, regulatory guidance varies considerably, ranging from enforceable rules for specific sectors to voluntary guidelines with limited oversight.

A significant proportion of firms remain outside the direct reach of regulation, either due to their geographical location, sector, or business model. Yet given the operational, reputational, and financial risks associated with IT incidents, these firms cannot afford to wait for regulation to compel action. Proactivity is the name of the game.

Businesses can draw from established industry frameworks as the foundation for their approach to managing IT risk. One route is to look to regulated peers for best practices, another is to reference widely recognized standards, such as the NIST Cybersecurity Framework (CSF).[2]

NIST CSF 2.0

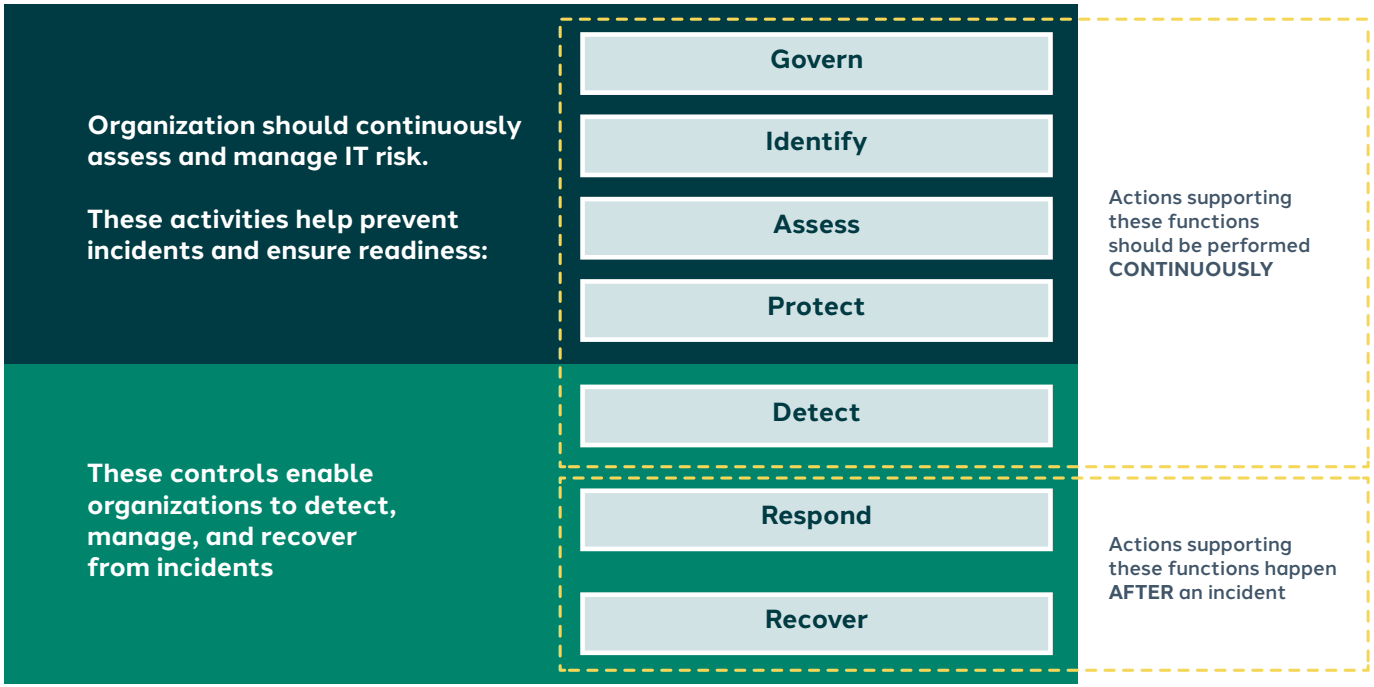
The NIST CSF is widely adopted as a foundational standard for managing IT and cyber risk, particularly among organizations that are not subject to strict sector-specific regulations. It offers a flexible, risk-based approach that can be tailored to different operational contexts, providing clear guidance on how to identify, protect, detect, respond to, and recover from cyber threats. This adaptability makes it an ideal starting point for building or enhancing IT risk management frameworks in a way that is both practical and scalable.

For highly regulated sectors, the NIST CSF serves a complementary role. While regulatory obligations may require adherence to specific controls or frameworks, the NIST CSF can help firms benchmark their existing practices, identify gaps, and strengthen their overall security posture. It serves as an additional lens through which to assess and mature cybersecurity capabilities, ensuring coverage of best practices that may go beyond or reinforce sectoral regulations.[3]

End-To-End IT Risk Management

The NIST CSF addresses the entire risk management lifecycle, from identification to recovery, encompassing both risk management and resilience. Below, we outline and expand on its key components as a foundation for executing a comprehensive IT risk management strategy.

2. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf
3. The NIST CSF is not a substitute for full regulatory compliance, nor does it cover all requirements imposed by regulations like NIS2, DORA, or sector-specific mandates.



Adapted from: NIST

- **Govern:** Define and oversee your risk management strategy, policies, and roles. Governance ensures that risk management aligns with the organization's objectives and that security priorities reflect stakeholder expectations.
- **Identify:** Develop a deep understanding of your business context, critical assets, and supply chain. Map all critical operations to the internal systems and external service providers that support them. Maintain an up-to-date inventory of assets, data, and dependencies that could impact business continuity. A dynamic risk register should capture relevant threats and vulnerabilities (e.g., the latest OWASP Top Ten) while also accounting for unique risks specific to your organization.

- **Assess:** Evaluate the likelihood and potential impact of disruptions on each critical process. This involves conducting risk assessments and due diligence on both internal systems and third parties. Consider inherent risk factors, then account for existing controls and service level agreements to determine residual risk. The assessment should also define the amount of downtime or disruption each process can tolerate under various scenarios.
- **Protect:** Implement appropriate safeguards to limit or contain the impact of potential incidents. This includes technical controls (access management, encryption, and backup systems), process controls (change management and secure development practices), and people controls (security awareness training and incident response planning).
- **Detect:** Continuously monitor systems, networks, and activities to identify anomalous behavior, attacks, or failures. Use a combination of real-time monitoring, automated alerting, and periodic testing (e.g., vulnerability scans, penetration tests) to verify that protective measures are functioning and that new risks have not emerged beyond your risk appetite.
- **Respond:** When a threat or incident is detected, take coordinated action to contain the incident, eradicate the threat, and inform stakeholders. A well-defined response plan should outline roles and communication protocols (including with executives, customers, regulators, etc.) during a cyber event.
- **Recover:** Rapidly restore any capabilities or services impaired by cybersecurity incidents, returning to normal operations as quickly as possible. Prioritize restoration of systems based on their criticality as identified in the Identify phase. The recovery phase also includes public communications and post-incident analysis.

A Lack of Visibility is Undermining Your IT Risk Framework

Implementing an IT risk framework is challenging in practice when organizations lack visibility into the very assets and risks they are trying to manage. Today, most enterprises struggle with fragmented views of their IT environment due to a few pervasive issues:

- Multi-layered vendor ecosystems
- Legacy systems and shadow IT
- Incomplete and inaccurate data

You can't manage what you can't see, and these challenges are compounded by the reliance on manual processes, which are prone to errors and become unsustainable over time.

Third-Party Dependencies

Third-party and fourth-party relationships are a major blind spot for many organizations, not least because of the sheer number of vendors firms deal with, but also because of the nuanced nature of those relationships.

A provider might be classified as “material” to an organization’s operations in several ways. Sometimes, the materiality is clear-cut: if a single contract or service is critical to business continuity, such as an IT provider managing core banking systems, that one arrangement is enough to make the provider material.

But more often, the risk lies in less obvious, cumulative dependencies. A service provider may handle multiple functions, such as network management, customer support, and data storage, that, taken individually, don’t classify as essential. However, when combined, these dependencies create a level of operational risk that makes the provider material to the business.

Legacy Systems and Shadow IT

InfoSec teams often manage a mix of modern and legacy systems within the enterprise. Older systems may not produce the necessary logs or metrics for demonstrating compliance, yet they still run critical parts of the business.

Additionally, shadow IT (unsanctioned apps or cloud services adopted by business units) can escape the purview of InfoSec, leading to pockets of non-compliance. Traditional compliance frameworks don’t account for the dynamic nature of IT today, including cloud resources spinning up/down, continuous software deployment, and more. The result is that the InfoSec office is always chasing a moving target with legacy approaches, and by the time they document compliance for one system, the environment has changed.

Incomplete and Inaccurate Data

Most organizations lack the complete and reliable data they need to understand their IT risk landscape fully. Critical information is scattered across spreadsheets maintained by different business units, incompatible security and compliance tools, and legacy systems that lack robust logging and reporting capabilities. In many cases, foundational data wasn’t collected or standardized in the first place, especially from third-party suppliers or shadow IT.

This fragmented approach means InfoSec teams are forced to piece together evidence from disparate sources, often in inconsistent formats and with significant gaps. Key details, such as system configurations, vendor dependencies, or real-time security control status, may be missing, outdated, or inaccessible.

The Future: A Consolidated, Intelligent Framework

Connection is collaborative and reciprocal. Stakeholders must collaborate to collect and share the right data, and then work together to interpret and act on that data.

GRC platforms enable a more connected, data-driven approach to IT risk management.

Three foundational shifts define this future:

1. **Centralize risk data:** Organizations must break down silos and achieve a unified, real-time view of risk across all departments. This means teams working together to map processes, standardize data, and feed a dynamic centralized system for risk management.

2. **Focus on risks before controls:** Make risk the primary focus, not a checklist of controls. Traditional programs often have been control-driven, rather than risk-driven, meaning they focus on ticking off control requirements without thoroughly assessing whether critical risks are truly mitigated. This can lead to blind spots or over-investing in controls that don't address the most significant risks. A modern GRC platform centralizes risk registers and analysis, allowing teams to prioritize remediation based on risk severity rather than just compliance tasks.

3. **Produce contextual intelligence for decision-makers:** IT risk outputs must be translated into business-friendly insights that drive informed decisions at every level. It's not enough to collect data; the findings must be accessible and contextualized for executives and non-technical stakeholders. Modern risk dashboards and reports are therefore designed to speak the language of the C-suite, directly connecting IT risks to business impacts like enterprise value, strategic priorities, and resilience objectives.

SAI360 empowers InfoSec leaders to move beyond silos and manual workarounds. Its integrated GRC platform unifies data, automates evidence collection, and centralizes risk registers, offering real-time dashboards tailored for both technical and business audiences. SAI360 enables you to break down organizational barriers, operationalize leading frameworks, and foster a culture of shared accountability, turning day-to-day risk management into a source of strategic strength.

Our unified approach to risk sets us apart

Today's complex risk landscape demands more. SAI360 leads the way with an integrated GRC platform that spans the entire risk and compliance spectrum.

- Whistleblower and Case Management
- Ethics & Compliance Training
- Policy Management
- Conflicts of Interest
- Incident Management
- Regulatory Compliance
- Regulatory Obligations
- Horizon Scanning
- Enterprise & Operational Risk Management
- Third-Party Risk
- Internal Audit
- Internal Controls
- IT Risk
- Business Continuity
- Vendor Risk Management