XM Cyber

Whitepaper

From Reactive to Resilient

Navigating the New Era of Cyber Compliance

Contents

Executive Summary

- **Compliance is now a frontline business priority** - It has shifted from a back-office function to a core driver of resilience, trust, and competitive positioning.
- **Point-in-time compliance is no longer sustainable** - Periodic audits and manual reviews can’t keep up with real-time threats or regulator expectations.
- **Tailored frameworks are replacing one-size-fits-all models** - Custom compliance strategies ensure relevance, efficiency, and scalability in complex operational environments.
- **New regulations are raising the stakes in 2025** - Frameworks like NIS2, DORA, the SEC cyber rules, and AI-specific legislation are expanding scope, shortening timelines, and increasing enforcement.
- **Continuous compliance is the new standard** - Automation, integration, and real-time monitoring enable organizations to detect and remediate issues before they become violations.
- **Emerging technologies create new challenges** - Developing technologies like AI, ML, and predictive analytics demand governance at the design stage to ensure both compliance and security.
- **Global organizations face overlapping and conflicting requirements** - Navigating the divide between mandatory and voluntary standards requires clarity, coordination, and strategic prioritization.
- **Compliance must be built into the workflow** - Policy-as-code, DevSecOps alignment, and cross-functional accountability are now standard for modern compliance programs.
- **A structured action plan sets the foundation for resilience** - From gap analysis to solution partnerships, organizations that act now will be better prepared for what's next.

The Compliance Wake-Up Call

Compliance isn't a back-office task anymore - it's at the heart of how organizations manage risk, ensure resilience, and build trust. For years, it was treated like a checkbox - something to handle once a year for the auditors. That era is over.

Regulators, partners, and customers now expect more - and so do boards, insurers, and investors. Governments have tightened frameworks, shortened timelines, and stepped up enforcement. Security and compliance can't wait for audit season - because threats and threat actors don't. And when compliance slips, the fallout is bigger than fines. Noncompliance today carries real-world business impacts - downtime, reputational damage, lost customers.

Organizations are feeling the pressure. Stakeholders want proof of ongoing security. Boards want clear oversight. Investors ask how risk will scale. And yet, many teams are still using outdated tools and reactive processes - relying on manual audits and snapshots that can't keep up.

Cyber risk shifts by the hour. Compliance needs to do the same. This is the compliance wake-up call.

This white paper explores why compliance must evolve into a continuous, adaptive process - one that strengthens resilience, accelerates response, and supports broader security goals.

The Regulatory Surge – What's New in 2025

The regulatory landscape has grown more complex, aggressive, and interconnected. In 2025, we're seeing a wave of new rules and updated standards that aim to address emerging cyber risks, expand sector coverage, and tighten reporting expectations. These aren't just legal checkboxes - they are active indicators of where regulators expect organizations to focus their efforts. Below is a look at the most impactful changes shaping compliance programs this year.

NIS2 (EU Network and Information Security Directive)

In 2025, the EU's NIS2 Directive enters enforcement, expanding cybersecurity requirements across critical sectors like healthcare, finance, and digital infrastructure. Stricter breach reporting, risk management, and supply-chain security are now mandatory. Regulators will prioritize cross-border coordination, with enforcement actions in 2025 expected to shape compliance expectations and disclosure standards.

DORA (Digital Operational Resilience Act – EU)

In 2025, the EU's Digital Operational Resilience Act (DORA) came into effect, imposing stringent cybersecurity mandates on financial entities (banks, insurance firms, investment companies and more) and their critical technology service providers. These organizations must establish comprehensive cyber risk management frameworks, conduct regular resilience testing, and report significant incidents. Additionally, DORA enforces strict oversight of third-party providers, requiring financial entities to manage associated risks diligently. Noncompliance may result in substantial penalties, including fines up to 2% of global turnover for financial entities and up to €5 million for critical service providers.

SEC Cybersecurity Disclosure Rules (U.S.)

In 2025, public companies must comply with the SEC's cybersecurity disclosure rules, effective since December 2023. These rules require companies to report serious cybersecurity incidents within four business days after deciding the incident is significant. Additionally, annual reports must detail the company's cybersecurity risk management, strategy, governance, and board oversight processes. This makes board-level cybersecurity oversight a formal, scrutinized component of regulatory requirements.

EU AI Act

In 2025, the EU's AI Act begins enforcement, introducing a risk-based framework for AI regulation. High-risk AI systems in sectors like healthcare and security must meet stringent requirements for transparency, safety, and bias mitigation. Organizations are mandated to conduct comprehensive risk assessments and establish governance processes. Certain AI practices, such as social scoring and specific biometric surveillance, are prohibited. The Act's implementation is phased, with bans on unacceptable-risk AI systems effective from February 2025, and full compliance for high-risk systems required by August 2027.

ISO/IEC 27001:2022

In 2025, organizations are expected to have fully integrated the enhancements introduced in ISO/IEC 27001:2022, which became effective in October 2022. This version introduced 11 new controls focusing on areas such as threat intelligence, cloud service security, physical security monitoring, and data leakage prevention. Organizations certified under ISO/IEC 27001:2013 are required to transition to the 2022 version by October 2025 to maintain their certification status.

UK Cyber Security and Resilience Act (CSRA)

In 2025, the UK's Cyber Security and Resilience Bill (CSRA) is set to enhance oversight of foreign firms operating in the UK, introducing stricter incident reporting requirements and expanding regulator powers for audits and penalties. Organizations must prioritize digital trust, ensure data integrity and secure interactions to comply and avoid penalties. Adopting scalable security frameworks and collaborating with trusted service providers will also be crucial for compliance.

Canada's CPPA (Consumer Privacy Protection Act)

If enacted in 2025, Canada's Consumer Privacy Protection Act (CPPA) will replace the Personal Information Protection and Electronic Documents Act (PIPEDA) from 2021, strengthening individual rights and organizational responsibilities. It will mandate greater transparency, especially around automated decision-making, and give individuals more control over their personal data. Organizations will need to update privacy programs and ensure clear, accountable data practices.

GDPR (EU General Data Protection Regulation) **Updates**

Enforcement of GDPR continues to ramp up in 2025, with regulators placing greater emphasis on cross-border investigations and coordinated oversight. Authorities are particularly focused on how organizations handle emerging technologies such as artificial intelligence, automated decision-making, and behavioral profiling. At the same time, proposed reforms aim to streamline GDPR compliance for small and medium-sized enterprises, in an effort to balance robust data protection with business competitiveness. Organizations should be prepared for both stricter enforcement and evolving expectations as the European Commission works to modernize the regulation without weakening its core protections.

NYDFS Cybersecurity Regulation (New York)

Many of the stipulations in the NYDFS Phase 2 take effect in 2025. Notably, larger firms will face added steps like audits and weekly scans, while all organizations must improve board oversight and give CISOs more authority. Key deadlines in April, May, and November mandate stronger access controls, MFA, asset inventories, and incident response.

HIPAA Refinements (U.S.)

Proposed 2025 updates aim to modernize HIPAA by strengthening cybersecurity requirements, including encryption and multifactor authentication. The changes also push for improved patient access to electronic health records through standardized APIs and clearer interoperability standards. Regulators are increasing penalties for noncompliance, reflecting growing concerns over healthcare data breaches and third-party sharing risks. As digital threats evolve, covered entities must reassess their security practices and update compliance programs to meet the new requirements. The updates mark a shift toward more proactive, tech-aware enforcement of HIPAA in today's connected healthcare environment.

PCI (Payment Card Industry) **4.0**

On March 31, 2025, requirements 6.4.3 and 11.6.1 under the PCI Data Security Standard (PCI DSS) came into effect, impacting many merchants processing online payments. PCI Compliance outlines a set of requirements for securing credit card transactions and protecting cardholder data. Any merchant processing, storing, or transmitting credit card information should comply with PCI and organizations that aren't compliant may be fined up to $500,000 per incident. Companies also must notify each person who might have been exposed in an attack.

From Point-in-Time to Continuous Compliance

For years, compliance was treated as a fixed event – a quarterly or annual milestone to be checked off during audit season. This point-in-time approach worked in a slower world. But today, it's out of step with reality. Cyber threats move fast, vulnerabilities are discovered daily, and regulators are tightening timelines and expectations. A yearly checklist simply can't keep pace.

Today's compliance needs to be dynamic. Continuous compliance is the shift from reactive, snapshot-based assessments to an always-on, integrated approach. It means compliance isn't something you prepare for once a year – it's something you maintain every day. And this isn't just about checking a box more frequently. It's about changing the entire approach to managing cyber risk and aligning it with operational realities.

As outlined in Forrester's 2024 report, No More Blurred Lines: Introducing Continuous Risk Management, the traditional "Three Lines of Defense" model has reached its limit. It offers a governance structure, but not a functioning risk management process. In its place, Forrester proposes a more actionable alternative: an eight-phase Continuous Risk Management (CRM) model that reflects how risk and compliance actually unfold - across time, teams, and technologies.

The 8 Phases of Continuous Risk Management

Forrester replaces the rigid Three Lines of Defense with a more agile, eight-phase model designed for continuous, real-time compliance. These phases help organizations align risk management with strategic decision-making, operational execution, and rapid response.

1. **Identify the Opportunity or Business Need**
   Define the value you're pursuing and what's at stake.
2. **Plan Risk Strategy and Governance**
   Set risk objectives, stakeholders, and governance early.
3. **Analyze Context and Feasibility**
   Validate the plan against organizational realities and risk exposure.

The Forrester model shifts the emphasis from what standard you follow to how you implement and sustain it. It lays out a step-by-step process that starts with identifying business priorities and planning for risk — then continues to ongoing monitoring, control validation, and measurable outcomes, all tied directly to organizational goals.

Organizations adopting this approach gain more than regulatory coverage. They build resilience into their day-to-day operations, reduce the cost of noncompliance, and create a foundation for faster, more informed decisions. Continuous compliance becomes a function of continuous risk understanding - supported by automation, real-time validation, and adaptive governance.

Modern compliance is always on, always improving, and always connected to the bigger picture. But getting there requires the right tools. Organizations need to seek out platforms that support this shift. It’s not enough to hope your old systems will keep up. Continuous compliance demands continuous capability.

4. **Design the Mitigation Approach**
   Choose which risks to accept, mitigate, or transfer and how.

5. **Implement Controls**
   Deploy controls across systems, teams, and third parties.

6. **Respond to Deviations**
   Detect, test, and adjust controls when issues arise.

7. **Measure Control Effectiveness**
   Use key indicators to track performance and outcomes.

8. **Monitor and Communicate Continuously**
   Share insights, escalate when needed, and update as conditions change.

What Continuous Compliance Looks Like in Practice

Continuous compliance isn't just a mindset shift - it's a set of tangible, integrated practices that operate in real time. In practice, it means embedding compliance into the day-to-day workflows of security, IT, and development teams. It's no longer a box to tick during audit season – it's part of how the organization runs, every day.

At the core is **automated monitoring.** Tools continuously scan cloud configurations, access controls, data flows, and system activity for misalignments with compliance frameworks. When something drifts out of scope - like an unpatched system or an insecure API - alerts are triggered, and remediation can begin immediately.

Policy-as-code is another key element. Compliance rules are defined in code and built into CI/CD pipelines, ensuring that every infrastructure change is evaluated before it goes live. This helps DevOps teams move quickly without creating risk.

Real-time evidence collection replaces the scramble of manual audits. Documentation is updated automatically, making it easy to respond to regulator requests or internal reviews on demand.

And finally, **integration across teams** is essential. Compliance isn't owned by one function - it's shared by security, engineering, legal, and operations. Everyone contributes, and everyone is accountable.

This kind of cross-functional accountability is exactly what Forrester's continuous risk management model calls for — integrating compliance efforts across business, technical, and governance layers in a repeatable, adaptive loop. This is what modern compliance looks like - automated, continuous, and embedded across the organization.

The Future is Flexible – Tailored Frameworks

A one-size-fits-all approach to compliance no longer holds up. Organizations face vastly different risks, regulations, and operational realities depending on their industry, geography, and structure. To meet this complexity head-on, many are turning to tailored compliance frameworks - purpose-built controls and processes aligned to specific business needs.

Custom frameworks deliver several clear benefits:

Relevance

Controls are aligned with actual exposure and regulatory scope. For example: A fintech startup focuses on PCI DSS and anti-money laundering rules, rather than applying healthcare or manufacturing standards.

Efficiency

Resources are directed where they matter most.
For example: A manufacturer replaced redundant ISO controls with NIS2-focused measures targeting third-party risk.

Scalability

Frameworks evolve with the organization.
For example: A US-based healthcare group expanded its HIPAA program to include GDPR when it began serving European clients.

Designing a tailored framework starts with assessing the organization's risk profile, business model, and regulatory obligations. This often involves mapping existing controls to multiple standards, identifying gaps, and integrating relevant best practices into a cohesive program.

Emerging Technologies and Their Compliance Impact

New technologies are reshaping how organizations approach compliance. While they offer powerful new capabilities, they also introduce fresh risks and regulatory gray areas that are still coming into focus.

Artificial Intelligence (AI)

AI enables faster decision-making, real-time monitoring, and better anomaly detection. But it also raises concerns around explainability, accountability, and ethical use - particularly in finance, healthcare, and hiring.

Generative AI and LLMs

Tools like large language models can speed up reporting, documentation, and development. But they also carry risks - from hallucinated content and IP leakage to accidental exposure of sensitive data.

Machine Learning (ML)

ML can flag suspicious behavior and refine risk models, but without proper oversight, it may reinforce bias, produce opaque decisions, or compromise privacy - especially when training data lacks transparency.

Predictive Analytics

Predictive models help prioritize risk and guide proactive controls. Yet regulators are paying closer attention to how these models are developed, validated, and explained - particularly in high-stakes industries.

To navigate this complexity, many organizations are adopting compliance-by-design - building governance, transparency, and risk controls directly into the development and deployment of new technologies.

Action Plan for 2025 and Beyond

As regulations grow more complex, organizations need a clear and proactive approach to stay compliant. The following is a solid starting point for building a structured compliance strategy:

☑ Assess your current compliance

Start with a gap analysis. Review your existing policies and practices against relevant regulations to spot areas of risk or non-compliance. Structured templates can help ensure nothing gets missed.

☑ Create a modernization roadmap

Outline a practical plan to close those gaps. Set timelines, assign resources, and prioritize actions. Where possible, align with models like Forrester's eight-phase framework to ensure your roadmap supports continuous, risk-driven compliance.

☑ Build a compliance-driven culture

Make compliance part of your organization's day-to-day. Offer regular training and communicate expectations clearly. A culture of accountability and ethical behavior reduces the risk of violations.

☑ Work with external experts

Regulations change fast. Partnering with compliance solution providers gives you access to specialized tools and up-to-date knowledge - helping you stay ahead of new requirements.

This sample framework can help guide early efforts - but sustained compliance requires ongoing review, adaptation, and commitment across the organization.

XM Cyber Helps Organizations Effectively Achieve Continuous Compliance

Compliance is no longer a checkbox exercise - it's an ongoing effort that demands speed, flexibility, and coordination. With new laws like NIS2, DORA, and the SEC cyber rules now in effect, and others like the EU AI Act and CPPA close behind, the expectations are higher and the timelines shorter.

Point-in-time audits and generic frameworks are no longer enough. To stay ahead, organizations need continuous, adaptive compliance that's embedded in day-to-day operations - powered by automation, shared across teams, and aligned with business priorities.

In this new compliance climate, the organizations that will thrive are those that treat compliance not as an obligation, but as a strategic advantage - one that strengthens resilience, supports innovation, and builds lasting trust.

XM Cyber is leading the way in helping organizations use this evolving compliance ecosystem as a springboard for growth. It grants the ability to continuously enhance security posture through the unification of security intelligence, evaluate the effectiveness of the security stack, and optimize defenses against persistent threats. Moreover, organizations can simulate real-world breaches, get continuous control validation, and automate reporting. The full suite of compliance-focused capabilities means that no matter what regulation or requirement comes next, your organization can address it comprehensively.

The Bottom Line

Close the gap between compliance policy and practice, strengthen resilience, and build lasting trust across the business. With XM Cyber, your compliance program will always be ready for whatever requirement or framework comes next.

Want to prepare for whatever's next on your compliance journey? Grab our best practices checklist here!