

kyndryl.

Regulation Readiness

Preparing for Global
Cyber Rules



Table of Contents

01

Introduction

02

Cyber Regulation in Context

03

Cyber Regulation Activity

- Americas
- Europe
- Asia

04

Kyndryl's Perspective

- Ability to Bounce Back
- A Commitment to Transparency
- Staying Prepared
- Keeping an Eye on Protection

05

The Enterprise Leaders Involved

06

Implementing Cyber Regulation Readiness

- Experienced Experts
- Proven Partnerships
- Emerging Technologies

07

Summary

Have questions?

Contact our Corporate Affairs team for additional guidance:

- **Global Policy** – Fariba Wells (fariba.wells@kyndryl.com)
- **Cyber Regulation** – Alex Lau (alex.lau@kyndryl.com)
- **Thought Leadership** – Chase Purdy (chase.purdy1@kyndryl.com)

Introduction

As the world's largest managed infrastructure services provider, Kyndryl has a unique perspective on emerging technologies and the global forces that shape how they are deployed.

The world — and its digital infrastructure — is growing more complex and more quickly than ever before. To that end, the need for a steady hand and experienced advisor is more important than ever as enterprise technology leaders and governments seek to navigate a challenging IT landscape. At Kyndryl, we see this moment as an opportunity for great progress — a chance to show up for our customers when, where, and how they need us.

With the growing digitization of the global economy, there's been a corresponding increase in cyber threats, including cyberattacks, data breaches, and other malicious activities targeting digital systems, services, and critical third-party providers that support them. Many digital services, especially those in sectors such as finance, are connected. A cyber incident in one service provider can have cascading effects that can lead to systemic risks for an entire digital ecosystem. With that in mind, nations are seeking to curb those risks through regulation.

Globally, the landscape of regulations remains fragmented, even if the shared goal is to address evolving challenges and risks associated with the digitization of the economy. To that end, Kyndryl launched a campaign designed around **cyber regulation readiness** as a means of assisting enterprises through a consultative approach as they look to comply with new rules while maintaining focus on their overarching business strategies and ambitions.

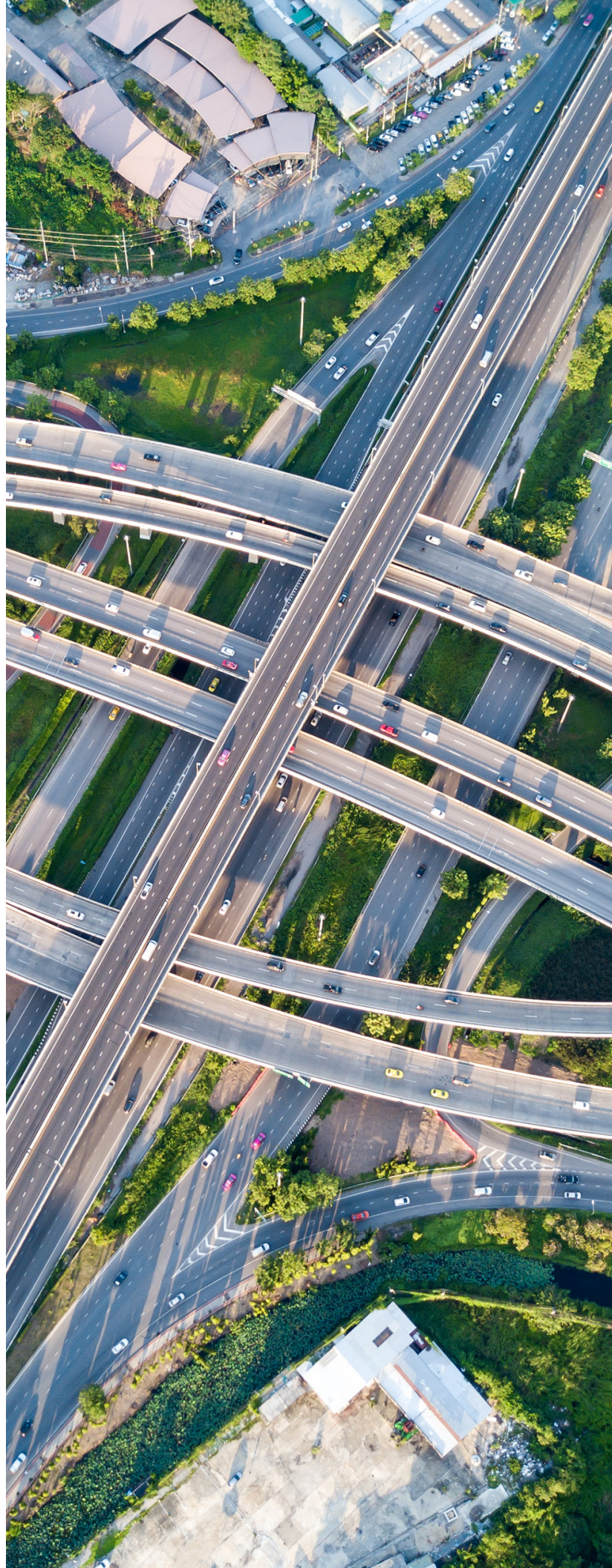
At Kyndryl, we:



Understand that a contemporary cybersecurity strategy must be one that embraces the idea of cyber resilience. The ability to anticipate, protect against, withstand, and recover from any cyber-related event is paramount in a threat environment that all but assures some attacks will cause disruption.



Support our customers as they navigate a complex and evolving regulatory landscape. Globally, governments are addressing rising risk with regulation to augment focus on governance, risk, and disclosure. That's adding pressure to enterprises who seek to maintain smooth business operations and comply with new rules.





Cyber Regulations in Context

In the last decade, enterprises everywhere have undergone intense digital transformations. This led to innovations in service delivery, operations, and customer engagement. In short, it opened new markets and opportunities for growth.

But that increase in the digital landscape also led to a corresponding increase in cyber threats as bad actors found more opportunities to exploit enterprises. Working to navigate the complexity of the threat environment, as well as a patchwork of regulatory compliance requirements across the world, can be a thorny proposition.

Consider a large financial institution as an example. A challenge today is that bad actors aren't just going after the bank itself

— they're also looking for ways to exploit critical third-party providers of services to the banks. That's because attackers know the easiest, fastest way to get into those organizations is through the supply chain. Maybe the bank has a marketing team that has hired an outside firm to help with promotional campaigns. It's now easier for bad actors to target those outside firms, integrating malware into those organizations that allows them to sneak into the bank, which could lead to a ransomware attack, among other things.

In response to this new array of challenges, some governments are adopting new regulatory frameworks to bolster enterprise security.

71%

of respondents reporting they've experienced a cybersecurity-related incident.

84%

agreed or strongly agreed that their organization relies heavily on IT assets to operate critical business processes.

50%

of respondents who experienced an attack, reported their business operations were disrupted.

Cyber regulations can be beneficial for the global economy. They establish a standardized framework for cybersecurity and data protection, both of which foster trust and confidence in digital transactions and services. By requiring enterprises to adopt robust security and resiliency measures and to manage cyber risks effectively, these regulations help mitigate the potential for significant financial losses and disruptions. This, in turn, promotes the stability and resilience of global financial markets and supply chains.

While much of that may sound like common sense, it should not betray the immense challenges ahead of global enterprises as they seek to comply with new regulations – especially when they exist across the globe in a non-congruent patchwork.

Consider again the impact of new cyber regulations on a large, multinational financial institution that has operational footprints around world. It is a challenging and complicated task to comply with multiple regulatory standards – some that are similar, and some that are not. And just because the enterprise's headquarters might be based in a country that does not have a cyber policy does not necessarily mean that it, or its customers, aren't affected.

Cyber Regulation Activity



Americas

- December 2023 ● In the United States, the Security & Exchange Commission enforces Cybersecurity Risk Management, Strategy, Governance and Incident Disclosure.
- H1 2024 ● OSFI's B-10 (Third-Party Risk Mgmt) and B13 (Technology & Cyber Risk Mgmt) updated guidelines go into effect.
- H1 2024 ● In Brazil, the introduction of the Cybersecurity Regulation & Cybersecurity Authority Bill.
- H2 2024 ● OSFI publishes final E-21 guidelines - Operational Resilience and Operational Risk Management.
- 2025 ● In Canada, regulators will enforce C-26 - Critical Cyber Systems Protection Act.



Europe

- January 2023 ● In the European Union, DORA and NIS2 enacted by the European Commission.
- H2 2024 ● In the European Union, there is an expectation that the following will be finalized: The regulatory technical standards for DORA; the risk management technical details for NIS2; the Cyber Resilience Act for connected products; an amendment to the Cybersecurity Act for Managed Security Services Certification; and the Cyber Solidarity Act to create and EU-wide cyber response framework.
- October 2024 ● In the European Union, member states enforce NIS2.
- January 2025 ● In the European Union, ESAs enforce DORA; and in the UK, the Bank of England, FCA and PRA enforce Critical Third Parties for FS Sector and enforce Operational Resilience and Testing requirements.
- 2025 ● In the UK, the expectation of new legislation to update NIS Regulations to include MSPs.



Asia

- H1 2024 ● In Singapore, an expectation of the final text of amendments to the Cybersecurity Act.
- H2 2024 ● In India, expectation that the Digital India Act will move forward (including cyber requirements); also in Australia, there is an expectation that the regulators will move to strengthen existing regulations with a focus on critical infrastructure.
- 2025 ● In Japan, the Digital Agency is expected to propose draft cyber regulation, especially on incident reporting.

Future dates are tentative.

Kyndryl's Perspective

As governments and regulators begin debating, adopting, and enforcing new cyber resilience regulations, enterprises are increasingly being compelled to prioritize cyber security and resiliency spending. That's making the issue a top area of attention among enterprise technology leaders and the boardrooms to which they report.

To that end, there is an imminent need by enterprises to work with consultative partners who can provide perspective, expertise, and direction to help position them to **anticipate, protect against, withstand, and recover** from information and communication technology related disruptions and threats. Such a lens will prove invaluable when applied to such a complex challenge. Not all solutions can be applied straight out of a box.

~2,500

Kyndryl consultants with experience and training in security and resiliency.

7,000+

Security and resiliency certifications and accreditations held by Kyndryl experts.

568%

5-year ROI and 9-month payback period to investment in Kyndryl Security & Resiliency services.*

In general, there are four basic components that governments are interested in seeing enterprises can do within the framework of cyber regulations:

*Source: *The Business Value of Kyndryl Security & Resiliency Services*, IDC, July 2023

The Ability to Bounce Back

Regulators are keen to see enterprises take steps to ensure their Information and Communication Technology (ICT) systems are resilient. That can mean taking steps to implement measures to prevent, withstand, and quickly recover from disruptions — things like cyberattacks, technical failures, and natural disasters.

Key questions:

What do those steps look like?

- It can mean setting up processes for regular backups, implementing robust cybersecurity measures, developing effective incident response plans, and setting up a system for continuously monitoring for potential threats. And then there's the resilience aspect, which takes a realistic view of cybersecurity in that it anticipates some attacks will be successful, and that the top priority is to minimize downtime during such events while protecting data integrity and maintaining operational continuity even during those conditions.

A Commitment to Transparency

If an adverse incident does occur, regulators increasingly want to be informed. This is why many cyber regulations require enterprises to establish a structured process for incident reporting.

Key questions:

How do you know what needs to be reported, and by when?

- Typically, regulations lay out clearly defined guidelines as to what constitutes an incident that must be reported. These can include incidents of unauthorized access, data breaches, system disruptions, or other cybersecurity-related events. They also often set out deadlines of when you need to report it by. That can cause additional problems as the clock is ticking while you're working to figure out what is happening.

What does this kind of reporting entail?

- Firstly, regulators generally want enterprises to establish specific channels or platforms to report incidents. That can be through dedicated email addresses, online forms, or secure portals, for instance. Second, they want reporting to be timely. Regulations often mandate enterprises report incidents within a specific timeframe after discovery. That ensures the prompt notification of an incident to relevant stakeholders (regulators, customers, partners, etc.).

- As for the information that's shared, it typically involves laying out the nature and scope of the incident, its potential impact, the systems or data that were affected, and any efforts that were made to correct the issue.

Staying Prepared

Regulators want enterprises that are subject to cyber regulations to be especially cognizant of the risk landscape. That's why many of these rules come with specific requirements to assess risk, which involve systematically evaluating potential threats and vulnerabilities to the operational resilience of an enterprise's digital systems.

Key questions:

What does a risk assessment involve?

- There are several key components to a traditional risk assessment. It starts by first mapping out and understanding what critical digital assets, systems, and processes are potentially at risk. From there, enterprises need to consider what potential threats and vulnerabilities exist that could compromise the security and resilience of those assets. That could include cyberattacks, or technical failures, human errors, or even natural disasters.
- It's also important that enterprises develop mitigation strategies to reduce the likelihood and impact of an incident, as well as a response plan in the case something happens. Also important is establishing mechanisms for ongoing monitoring and reviewing — which helps teams adapt and refine their strategies as needed as the threat landscape continues to evolve.
- Some regulations involve testing readiness — not just assessing. Regulators want to know enterprises have a plan, that they've tested it, and that it works. They have to demonstrate they are able to effectively handle it.
- In addition to stipulating “what” organizations must assess risk for, regulations may also specify “how frequently” and “who” is conducting the assessment — all of which impacts overall enterprise operations, automation standards, etc.

Keeping an Eye on Protection

By maintaining robust cybersecurity measures, enterprises can enhance their digital cyber resilience. The process of continuously updating a set of practices and/or policies and technologies to protect digital systems is key.

Key questions:

How does this play out?

- The answer to this can quickly get into the weeds, as there are many nitty-gritty ways to advance this imperative. It can include implementing mechanisms to control access to sensitive data, such as user authentication steps and encryption. It can involve deploying endpoint security measures to prevent malware infections and data breaches. Setting up appropriate firewalls for network security and maintaining oversight over the lifecycle of data (including storage, transmission, and disposal) are also key, among other things.
- Also important to mention here are third-party risk assessments, which help manage cybersecurity risks associated with vendors, suppliers, and partners who have access to an enterprise's systems or data.



The Enterprise Leaders Involved

Within an enterprise, business and technical leaders must work together to prepare for, implement, and keep in compliance with evolving regulatory standards around the globe. While they share a single common mission, each role brings unique expertise and perspective to the issue.



Concerned with operational impacts of compliance with various cyber regulations. This can include the integration of regulatory requirements into day-to-day operations, the costs associated with compliance, and how compliance might impact the business processes, operational efficiency, and the overall bottom line.



Primarily focused on the technical and security aspects of cyber regulations, and how laws would impact their enterprise's information security management, data protection policies, cybersecurity tools, and overall resilience against cyber threats.



Focused on aligning technology strategy with regulatory requirements while also supporting innovation and technological advancement. At the end of the day, the CTO wants to ensure that compliance with regulations does not hamper innovation.



The CIO is responsible for overseeing an enterprise's overall information strategy, which includes in the management of information systems that support enterprise goals. Essentially, their interest is to ensure that enterprise IT remains compliant with regulations while also continuing to drive business value.



Their primary function in an evolving regulatory environment is to assess how changes impact the risk landscape and ensure that all types of risks related to compliance are identified and mitigated. This means aligning risk strategies with business objectives to protect and enhance value.

Implementing Cyber Regulation Readiness

The first step toward embracing a cyber resilient strategy and alignment with new regulatory frameworks is for enterprises to clearly define what they need to protect. That means scanning the overall business and considering the impact and implications across **operational, financial, reputational, and regulatory areas.**

Questions for When an Incident Occurs

- **Operational:** What other services are impacted by the absence of this service outage? Could this impact other critical organizations? How could this impact B2B customers and partners?
- **Financial:** What are the financial losses being accrued through certain services being down?
- **Reputational:** How will this impact customer loyalty? Will this impact the share price? How harmful is the downtime of this services to the customer experience?
- **Regulatory:** What level of scrutiny and potential fines will this outage bring from regulators?

Having a clear understanding of the parts of the business that underpin critical assets is critical to identifying threats and hazards and implementing mitigations.

This is often where a managed services and consultative partner can help, by identifying key components of an enterprise's critical infrastructure. That can include its systems, services, networks, people, information, and other key elements.

Step 1

Work with an experienced partner to identify and assess security and resiliency gaps. Chart a strategy for regulatory compliance.

Step 2

Implement solutions to comply with new regulations and improve operational resilience. This includes taking comprehensive approach to modernizing mission-critical IT infrastructure.

Step 3

Regulatory compliance and resilience strategy implemented. Process established for maintaining status quo.

Implementing required cybersecurity measures and protocols can be resource intensive. Some may even require significant investments in technology, training, and personnel. For enterprises that previously operated under less stringent or disparate regulations, aligning with comprehensive new frameworks can require modernizing existing systems and processes. This can be particularly onerous for smaller entities with limited cybersecurity expertise, who are not as prepared to interpret new regulations, let alone take on new operational challenges. The initial phase of compliance can sound daunting, requiring a concerted effort, strategic planning, and partnerships with third parties to help meet new regulatory expectations.

To help enterprises come into compliance with new regulations, IT leaders can leverage their response through the help of:

Experienced Experts

At Kyndryl, our people have decades of expertise in securing and recovering the most complex, mission-critical hybrid IT environments, and via our expertise and tooling, we can help assess business impact of key processes and model recovery efforts to compare against risk, and also support to assign quantitative and qualitative material risk to differing scenarios.

Further, we are actively influencing the global dialog on cyber regulations through our engagements with regulating bodies. Our experts are available to share their perspectives and their operational expertise.

Proven Partnerships

The most complex, mission-critical — and often regulated — IT environments and applications often require the most fulsome approach to modernization. It helps to have a comprehensive slate of solutions on hand. That is made possible through close alliances with hyperscalers and access to open integration platforms — such as Kyndryl Bridge — that offer unparalleled insight and overview of an enterprise's IT estate.

Emerging Technologies

Coming into compliance with new cyber regulations can be aided by powerful technological tools and solutions, including advances in secular trends that include artificial intelligence. When deployed in an advanced delivery setting, AI can continuously monitor and update standards and controls, making assessments based on risk, cost-effectiveness, and capabilities.



As a tool, it can be designed to provide a foundation of guiding elements, strategies, systems, and controls that agnostically support an enterprise's cybersecurity needs and priorities. It does this via threat protection and mitigation, as well as in helping to identify patterns of threats, alerting enterprise technology leaders to new threats that emerge, and discover patterns between cyber incidents.

Generally speaking, there are five main areas in which AI can fit as part of an enterprise's cyber regulation readiness strategy:

Threat Detection and Prevention — AI-powered cybersecurity systems can continuously monitor network traffic, detect anomalies, and identify potential security threats in real-time. By proactively identifying and mitigating risks, AI helps enterprises comply with regulations that require robust security measures.

Automated Compliance Monitoring — AI can streamline compliance monitoring by automatically scanning systems and data repositories to help make sure an enterprise is adhering to regulatory requirements. It can identify gaps and holes in security controls while also tracking potential policy violations and generating reports to demonstrate compliance to third-party auditors and regulators.

Risk Assessment and Management — AI-powered risk assessment tools can analyze huge amounts of data to identify potential vulnerabilities and assess their impact on compliance with cybersecurity regulations. Prioritizing risk based on severity and likelihood can help enterprises stop issues before they start and also guide important decisions around resource allocation.

Data Protection and Privacy Compliance — AI technology such as machine learning and natural language processing can help enhance data protection and privacy compliance efforts. They can help classify sensitive data, enforce access controls, monitor data use for compliance with privacy regulations, and detect data breaches.

Incident Response and Remediation — The ability to automate the detection, analysis, and remediation of security incidents, reducing response times and minimizing the impact of breaches are always ways AI can assist in keeping an enterprise compliant with cyber regulations. By swiftly containing and resolving security incidents, enterprises can mitigate compliance risks and fulfill reporting requirements more effectively.

Summary

As countries around the world adopt and implement cyber regulations, enterprises of all stripes must prepare to bring their operations into compliance and become more resilient. That work begins by identifying and working with an experienced partner to assess security and resiliency gaps, implementing solutions to comply with new regulations and improve operational resilience, and establishing a process for monitoring and addressing the ever-evolving threat landscape.

Enterprises that proactively work to get ahead of new regulations will improve their overall security posture, reducing the likelihood of falling prey to data breaches and cyber-attacks. This will serve to boost trust — and their reputations — among stakeholders, fostering stronger relationships with customers and partners. Moreover, staying ahead of compliance requirements also provides a competitive advantage, demonstrating a commitment to cyber security and data protection.

Overall, preparing for new cyber regulations is not only a regulatory necessity but also a strategic move that will yield numerous benefits and opportunities for enterprises.



© Copyright Kyndryl, Inc. 2024

Kyndryl is a trademark or registered trademark of Kyndryl, Inc. in the United States and/or other countries. Other product and service names may be trademarks of Kyndryl, Inc. or other companies.

This document is current as of the initial date of publication and may be changed by Kyndryl at any time without notice. Not all offerings are available in every country in which Kyndryl operates. Kyndryl products and services are warranted according to the terms and conditions of the agreements under which they are provided.