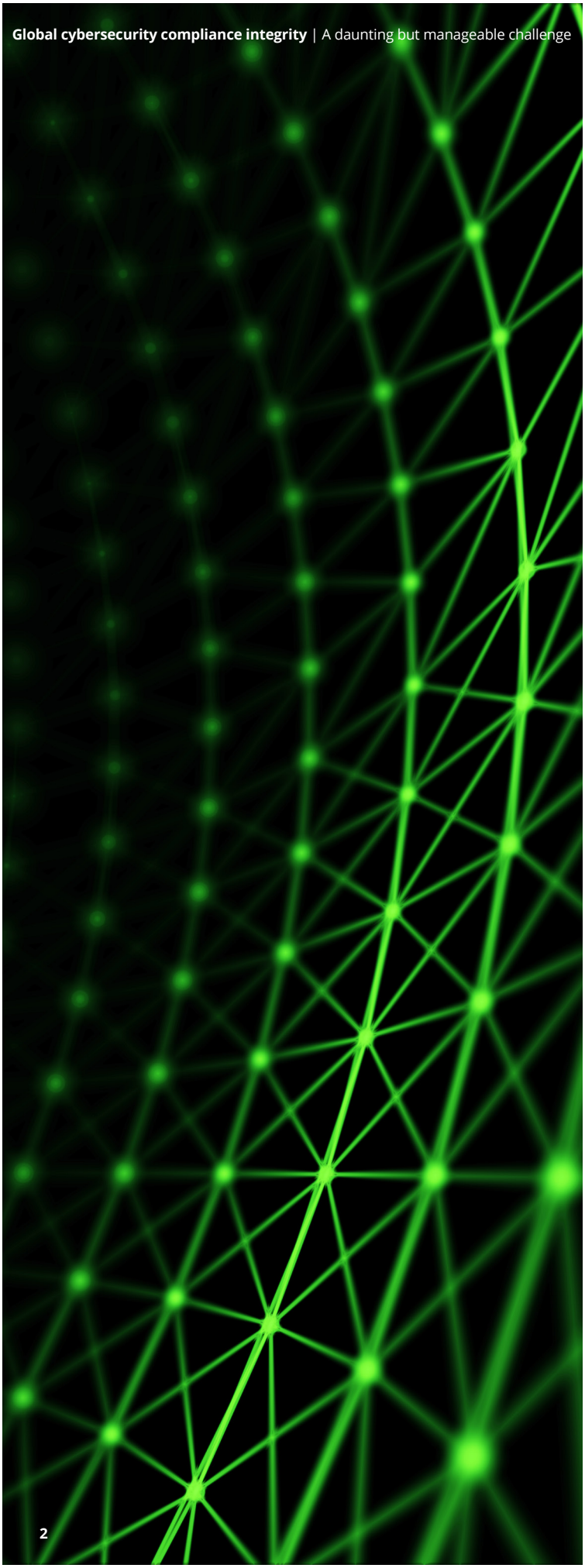
Deloitte.

Global cybersecurity compliance integrity

A daunting but manageable challenge

CENTER *for*
REGULATORY
STRATEGY
AMERICAS



Establishing an effective cybersecurity program is a major challenge for companies regardless of industry and geography. However, the challenge is much greater for businesses that operate internationally since they must comply with regulations from multiple jurisdictions and multiple regulators.

Although many companies already have programs in place to address cybersecurity risks, once formal regulations are established in different jurisdictions, companies should figure out how to achieve an efficient and effective control framework for global compliance.

The good news is that complying with the multitude of different regulations around the world is not as difficult as it appears to be. Although the regulations might look very different at first glance, a detailed comparison reveals many commonalities that can greatly simplify the task, allowing companies to lead in their industry, navigate risks and opportunities, and disrupt the status quo.

The challenge of global cyber compliance

Given how rapidly cybersecurity threats emerge and change, it can be hard for companies and regulators to keep up. The challenge is especially difficult for global companies, which should combat an endless stream of cybersecurity threats while demonstrating regulatory compliance in the jurisdictions in which they operate.

Companies based in countries that already impose rigorous cyber integrity requirements may have an edge because they have previously done a lot of the hard work required to clear a very high bar. On the other hand, companies based in countries with less rigorous requirements are likely behind on the compliance maturity curve and may thus need to work harder to catch up.

More similar than different

Fortunately, the similarity of requirements among global regulators makes the global compliance challenge much more manageable than it seems. Regardless of jurisdiction, many cyber regulations focus on the same or similar types of threats and vulnerabilities and require firms to adopt similar mitigating requirements, such as:

- Using a risk-based approach to understand the cybersecurity threats they face and implement a cybersecurity program that effectively addresses those threats
- Establishing a governance structure to drive accountability for the overall cybersecurity program
- Identifying systems that are subject to enhanced security controls
- Monitoring information systems for a breach or attempted breach of security
- Implementing formal incident and escalation programs to identify and respond to breaches and notify regulators and affected individuals in a timely manner
- Periodically testing the cybersecurity program

Many new cyber regulations are derived from existing regulations in more mature industries, such as financial services and banking. This process leads to themes and principles that become common across industries and geographies. When pursuing compliance, companies can learn hard-earned lessons from others. Also, many regulations are created with industry input, so they tend to reflect the needs, challenges, and constraints faced by real-world companies. That being said, regulators often make adjustments based on their own priorities and judgment, so companies don't always get what they ask for.

In addition, many regulations are closely aligned or directionally consistent with established or emerging standards, such as the National Institute of Standards and Technology (NIST) or the International Organization for Standardization (ISO). Implementing systems, processes, and controls based on such standards can help a company achieve compliance while demonstrating adherence to industry leading practices.

Example of regulatory similarities in banking

Around the world, various jurisdictions have established their own different regulations for cyber integrity in securities and banking. This example looks at three of the more prominent regulations—along with an industry standard (NIST)—to illustrate how hidden commonalities can ease the task of global compliance.

- **MAS TRM and Notice 644: Notice on Technology Risk Management[1] (Singapore).** This notice is issued pursuant to section 55 of the Banking Act (Cap. 19) (the Act) and applies to all banks in Singapore.
- **Interagency advanced notice of public rulemaking (ANPR) Establishing Information Security Standards (12 CFR Part 30[2]) (United States).** Regulatory agencies are considering applying enhanced standards to certain entities with total enterprise-wide consolidated assets of $50 billion or more.
- **New York State Department of Financial Services (NYDFS) Cyber Rule (23 NYCRR 500[3]) (New York).** This rule stipulates that each covered entity shall maintain a cybersecurity program designed to protect the confidentiality, integrity, and availability of its information systems.
- **National Institute of Standards and Technology (NIST) Cybersecurity Framework[4].** A standard framework for improving critical infrastructure cybersecurity.

1 Monetary Authority of Singapore (MAS) Notice 644.

2 Federal Register Proposed Rules for: Office of the Comptroller of the Currency, 12 CFR Part 30 [Docket ID OCC–2016–0016] RIN 1557–AE06, Federal Reserve System 12 CFR Chapter II [Docket No. R–1550] RIN 7100–AE 61, Federal Deposit Insurance Corporation, 12.

3 New York State Department of Financial Services Proposed 23 NYCRR 500.

4 https://www.nist.gov/cyberframework

Figure 1: Examples of cyber integrity regulations and standards in global banking

	Regulations			Standard
Requirements	MAS TRM and Notice 644	Interagency ANPR	NYDFS Cyber Rule	NIST
System classification				
Governance requirements				
Monitoring for cybersecurity events				
Recovery time objective (RTO)				
Incident response and reporting				
Definition of a security event				

Legend:
White = No requirement specified
Green = Requirements are broadly consistent
Yellow = Requirements are directionally consistent but may require special attention

As shown in Figure 1, although different regulations often use different terms and definitions, in practice most of the underlying requirements are actually quite similar and can generally be addressed through common actions.

For example, on the subject of system classification, each regulator has identified a classification of systems that are subject to the enhanced controls required by its regulations. The classification focuses on specific areas of risk the regulator is attempting to mitigate. In particular, for the regulations shown above:

- **MAS Notice 644:** MAS 644_02(01) defines a "critical system" as a system for which failure will cause "significant disruption to the operations of the bank or materially impact the bank's service to its customers, such as a system which (a) processes transactions that are time critical; or (b) provides essential services to customers. *System* means any hardware, software, network, or other information technology (IT) component which is part of an IT infrastructure."
- **Interagency guidelines:** "*Customer information systems* means any methods used to access, collect, store, use, transmit, protect, or dispose of customer information."
- **NYDFS Cyber Rule—Definition of information system:** "For purposes of this part only, the following definitions shall apply: 'Information system' means a discrete set of electronic information resources organized for the collection, processing, maintenance, use, sharing, dissemination or disposition of electronic information, as well as any specialized system such as industrial/process controls systems, telephone switching and private branch exchange systems, and environmental control systems."

In this example, although the exact definition of a system varies for each of the three regulations, client may need to classify systems using different criteria to ensure that enhanced standards, including monitoring and reporting requirements, apply to the appropriate systems. Firms may decide to rationalize various definitions in an effort to streamline compliance.

By contrast, an area where there is less consistency is incident response and reporting. Specifically, the MAS requirement has a four-hour response time objective, while NYDFS requires "prompt" recovery but doesn't define what "prompt" means.

- **MAS Notice 644:** "A bank shall establish a recovery time objective (RTO) of not more than four hours for each critical system. The RTO is the duration of time, from the point of disruption, within which a system must be restored. The bank shall validate and document at least once every 12 months, how it performs its system recovery testing and when the RTO is validated during the system recovery testing."
- **NYDFS Section 500.16 Incident Response Plan:** "As part of its cybersecurity program, each covered entity shall establish a written incident response plan designed to promptly respond to, and recover from, any cybersecurity event materially affecting the confidentiality, integrity or availability of the covered entity's information systems or the continuing functionality of any aspect of the covered entity's business or operations."

Here the requirements are directionally consistent but are different enough to require special attention and handling. In cases like this, one of the most stringent requirement typically becomes the default requirement; clear the highest bar and the rest are relatively easy to satisfy.

Although the illustrative example in Figure 1 only shows the commonalities between three specific banking regulations, similar levels of commonality can be found in other banking regulations around the world, including: the "General Principles for Technology Risk Management" from the Hong Kong Monetary Authority (HKMA); the "Cybersecurity Interpretive Notice" from the National Futures Association (NFA) in the US; "Comprehensive Guidance on Cybersecurity Controls" from the Hong Kong Securities and Finance Commission (SFC); and "Guidelines Related to Cybersecurity Framework" from the Reserve Bank of India.

Looking beyond banking, a similar pattern can be seen in other industries such as insurance and health care. In many cases, the commonalities in global regulatory requirements far outweigh the differences.

How to tackle the global compliance challenge

Here are some practical tips to help companies efficiently and effectively comply with cyber integrity regulations across multiple jurisdictions.

Think globally

Take a global view of cyber integrity regulations, developing and executing global strategies and plans to increase speed, efficiency, and consistency. Start by analyzing the cyber-related regulatory requirements for jurisdictions your business operates in, then establish a global framework that addresses the commonalities. Once that's done, you can create jurisdiction-specific approaches to handle remaining requirements.

Leverage standards

Because many regulations are at least partly closely aligned to established standards (e.g., NIST), those standards can be a valuable source of insights and synergies. In particular, they can give your company a head start on preparing for regulations that are still being developed, and can provide useful details that are often lacking in the regulations themselves. For example, cyber integrity regulations from the NYDFS require companies to conduct a risk assessment, but the regulations don't actually define what a risk assessment is. Companies can address this shortcoming by referring to the best practices contained in industry standards such as the NIST standard, which is closely aligned to the NYDFS regulation.

Established standards can also provide a starting point to help spot commonalities in various jurisdictional regulations that at first glance might seem very different. In fact, some organizations are actively encouraging regulators to map their requirements against existing standards. For example, the Risk Management Association had this to say about the Advance Notice of Proposed Rulemaking for Enhanced Cyber Risk Management Standards (the ANPR) issued by the Federal Reserve Board (Fed), Office of the Comptroller of the Currency (OCC), and Federal Deposit Insurance Corporation (FDIC): "We respectfully submit that the agencies consider clearly defining the relationship between cyber risk and information security in any forthcoming guidance or rulemaking and mapping any resulting guidance or regulation to the NIST Framework given that most, if not all, of the institutions which would be covered by such guidance or rule align with the NIST Framework."[5]

Fill the talent gap

Compliance with cyber integrity regulations requires deep experience in both technology and regulatory compliance. Although a growing number of companies are establishing a new function focused specifically on technology compliance, many of these fledgling organizations are still developing their capabilities and do not yet have the background and experience to fully tackle the complex challenges of cyber integrity regulation. This is particularly critical in the early stages of cyber integrity compliance—when global frameworks, strategies, and plans are being developed—since miscues in this startup period can lead to more serious problems down the road.

Help shape the rules

Companies can take advantage of opportunities to shape emerging regulations by providing comments to proposed rules—either directly or through trade groups—and by actively participating in conferences and other forums where influencers and decision makers are thinking about cyber integrity issues.

Daunting but manageable

Although complying with cyber integrity regulations across multiple jurisdictions sounds like a daunting challenge, in reality it is much more manageable than it seems. Although the various regulations might look very different at first glance, a close comparison of the detailed requirements generally reveals many commonalities that can greatly simplify the task. With the right subject matter knowledge and approach, global cyber integrity compliance is an achievable goal that is well within reach.

*****

This is the first in a series of Deloitte reports on cyber integrity. Future reports will take a closer look at specific regulations, industries, and geographies. They will also explore related issues such as data privacy, credit card regulations, and e-banking.

5 https://www.fdic.gov/regulations/laws/federal/2016/2016_enhanced_cyberrisk_3064-ae45_c-006.pdf

For more information

Authors

Susan Ameel
Managing Director | Deloitte Risk and Financial Advisory
Deloitte & Touche LLP
sameel@deloitte.com

Mike Prokop
Managing Director | Deloitte Risk and Financial Advisory
Deloitte & Touche LLP
mprokop@deloitte.com

Chris Spoth
Executive Director | Center for Regulatory Strategy, Americas
Managing Director | Deloitte Risk and Financial Advisory
Deloitte & Touche LLP
cspoth@deloitte.com

David Wilson
Independent Senior Advisor to Deloitte & Touche LLP
daviwilson@deloitte.com

Alex LePore
Senior Consultant | Deloitte Risk and Financial Advisory
Deloitte & Touche LLP
alepore@deloitte.com

Contacts

Emily Mossburg
Principal | Deloitte Risk and Financial Advisory
Deloitte & Touche LLP
emossburg@deloitte.com

Vikram Bhat
Principal | Deloitte Risk and Financial Advisory
Deloitte & Touche LLP
vbhat@deloitte.com

CENTER *for*
REGULATORY STRATEGY
AMERICAS

About the Center
The Deloitte Center for Regulatory Strategy provides valuable insight to help organizations in the financial services, health care, life sciences, and energy industries keep abreast of emerging regulatory and compliance requirements, regulatory implementation leading practices, and other regulatory trends.

Home to a team of experienced executives, former regulators, and Deloitte professionals with extensive experience solving complex regulatory issues, the Center exists to bring relevant information and specialized perspectives to our clients through a range of media including thought leadership, research ,forums, webcasts, and events.

Deloitte.