# A GC's Guide To Multijurisdictional Regulatory Compliance

By **David Dunn and Meredith Griffanti** (May 15, 2024)

David Dunn

Meredith Griffanti

Threat actors continue to launch cyberattacks with no signs of slowing down.

In response, governing bodies and regulatory agencies have attempted to address cybersecurity threats by continually introducing and refining regulation, largely aimed at requiring affected organizations to have protections in place to mitigate cyber risk and transparently communicating about incidents when they happen.[1]

However, simultaneously preparing for incidents and complying with these new regulations all over the world are challenging tasks. Add in organizations with a large geographical footprint involving different languages and cultural norms, connected subsidiaries, a vast customer base and endless suppliers, and this becomes even more daunting.

Overlapping regulation has created an increasingly fragmented and complex regulatory landscape with elevated oversight for organizations across the globe, especially as new legislation is introduced, such as the European Union's Cybersecurity Regulation, which came into force on Jan. 7.[2] Each of these regulations carries an associated risk of penalty, whether financial or otherwise, which need to be carefully considered when it comes to compliance obligations.

Managing the complexities of cross-regional cybersecurity regulation requires a best-in-class approach collaboratively led by the chief information security officer, head of compliance and general counsel: one that involves understanding the regulatory landscape, building a holistic compliance strategy, promoting collaboration and communication across borders, and ensuring ongoing evaluations and improvements.

**Cross-Regional Cybersecurity Regulation and Compliance**

For organizations operating in multiple jurisdictions, it can be arduous to decipher inconsistent cybersecurity rules across borders and regulatory regimes. The first step is identifying and understanding applicable regulation.

In the EU, this includes major legislation such as General Data Protection Regulation,[3] the Digital Operational Resilience Act[4] and the Digital Service Act.[5]

In the Americas, there are cybersecurity rules from the U.S. Securities and Exchange Commission,[6] cybersecurity requirements from the New York State Department of Financial Services,[7] the California Consumer Privacy Act[8] and the Health Insurance Portability and Accountability Act,[9] among others.

Hypothetically, a publicly traded organization with offices and customers across the globe, and that is in possession of customer data, including personally identifiable information, would be required to comply with the GDPR for its customers located in the EU, CCPA for customers residing in California, and the SEC cybersecurity rules as a company listed on the

U.S. stock exchange.

Each regulation carries its own set of obligations, and while there is potential overlap, maintaining compliance with one entity does not guarantee compliance across the board.

The GC has an integral role to play in the oversight and response to these regulatory challenges because of their understanding and oversight into legal issues, business operations and strategic goals of their organization, leveraging the chief information security officer to apply controls needed to reach compliance.

This knowledge and unique perspective places the GC into a vital role, responsible for ensuring regulatory compliance and protecting business interests, putting into stark context the ramifications of noncompliance.

## Holistic Compliance Strategy

Regulatory compliance is a risk management activity, and organizations can choose not to comply with requirements, accepting the risk of penalties or sanctions.

Once a decision is made on whether to move to a compliant state, the GC will advise on the implications of this decision, working with the chief information security officer and compliance teams to understand the aggregate risk of potential penalties and enforcement for noncompliance.

Individuals from different functions of the business, e.g., legal, communications, customer engagement/sales, IT/information security, risk, privacy, etc., can provide valuable insight and perspective on a comprehensive compliance strategy, and their input should be represented in a lean, cross-functional, core compliance team. The responsibility of this group is to work together on compliance efforts, but it should ultimately be driven and overseen by the GC and the chief information security officer.

By understanding the roles, expectations and resources needed from each business function, a comprehensive strategy can be developed, including accounting for cross-regional complexities, instead of tackling these challenges in an inefficient, siloed and piecemeal style approach.

After applicable regulation is identified and a multidisciplinary team is created, procedures for how to comply with cross-regional requirements should be developed. This involves de-duplicating the often overlapping requirements, followed by performing gap assessments, including assessing data governance protocols to understand what type of data is controlled, stored and processed across all regions of the organization.

A complete and deep understanding of an organization's data governance practices is needed to effectively manage regulatory complexities. Additionally, different regulatory requirements may lead to country-specific compliance efforts that result in deviation from the enterprise approach to security and data governance. Documenting these variances, and the associated risk presented to the organization, is vital to getting proper visibility into the risk posture of the organization.

The GC's role should also involve ensuring that the core compliance team creates a control development and revision strategy that helps to address recommended solutions and policy changes. Implementation is only effective if there is a well-thought-out plan serving as the foundation for alterations and additions. This process should also involve validating compliance efforts by conducting design and operating effectiveness testing.

Similar to a table-top exercise that simulates a real-world cybersecurity incident and identifies areas for improvement in an incident response plan, organizations should also test their regulatory strategies — and address any gaps discovered — on a regular basis.

In building a holistic regulatory strategy, GCs should outline various thresholds and decision-making protocols regarding compliance.

For example, how is materiality determined, and what are the organizations' thresholds for needing to disclose a cybersecurity incident to the SEC and other regulators? What other communications and reputational risks arise as a result of having to publicly disclose the incident? Or how does the GC ensure their external securities counsel and external cybersecurity counsel — if from different law firms — are on the same page?

Knowing the answers to these questions in advance is critical to maintaining compliance, especially in crisis situations where time — and quick decisions — are of the essence.

**Collaboration and Communication**

Transparency is key: Each team should be aware of what the others are working on and why.

GCs can help cultivate this mindset by highlighting that there is a common goal everyone is working toward, and it will only be reached through a collective effort, as well as why achieving compliance is important and necessary.

With new regulation regularly rolling out, and with updates to existing regulation continually being implemented, GCs should establish a clear way of communicating pertinent information across the organization, including across regions.

Further, GCs also need to fully integrate into existing processes, providing critical input into the decision-making process and considering what is needed to make a materiality disclosure, the implications of implementing the incident response plan, etc., to ensure the regulatory strategy is being managed in a collaborative and unified manner.

Results from FTI Consulting's "CISO Redefined"[10] survey revealed that one in three senior executives perceive their CISOs as being hesitant to raise potential vulnerabilities to leadership, with a similar proportion believing their CISO is making things sound more optimistic than reality. This presents a clear need for GCs to collaborate with CISOs and encourage open lines of communication, ensuring alignment on controls and risks so that leadership receives an accurate representation of the organization's threat profile.

**Ongoing Evaluations and Improvements**

Working toward compliance is not a static process.

GCs should implement continual mechanisms that monitor and evaluate the compliance strategy, e.g., policies, procedures and processes, allowing for adjustments and improvements as needed. Ongoing evaluation allows GCs to validate progress is maintained, meet key deadlines and confirm that the regulatory strategy is operating effectively.

In addition to maintaining current visibility of the cybersecurity strategy, GCs are encouraged to keep pace with cybersecurity threats that could affect the organization and ultimately disrupt compliance efforts or put the organization at risk of falling into noncompliance. This includes regularly meeting with the chief information security officer and external advisers for threat intelligence updates, and proactively ensuring that their knowledge is sufficient to understand and appraise risks facing the organization.

Ultimately, GCs should feel comfortable that the defensive posture managed by the chief information security officer is sufficient.

While certain regulatory requirements may remain static, for example, reporting a cybersecurity incident within X number of hours, variables that can affect compliance, such as how critical assets are secured, may not.

Controls vary over time too: As threats evolve and novel attack types emerge, the controls that are effective today may not be effective tomorrow. An agile compliance strategy is essential for properly managing the intricacies of cross-border cybersecurity regulation.

## Conclusion

GCs play a vital role in working with chief information security officers to form compliance readiness strategies and drive them forward efficiently. The regulatory landscape is constantly shifting, requiring GCs to be flexible and nimble in their approaches, especially when dealing with cross-regional implications.

A static response to cybersecurity threats risks exposes the organization to significant financial and regulatory risk.

But with a deep understanding of applicable regulation, a compliance strategy that was built holistically and is regularly reviewed and improved, and an environment where open communication is promoted, GCs can help develop a best-in-class approach to effectively manage the complexities of cross-regional cybersecurity regulation.

---

*David Dunn is head of Europe, Middle East, and Africa cybersecurity and senior managing director at FTI Consulting.*

*Meredith Griffanti is global head of cybersecurity and data privacy communications and a senior managing director at the firm.*

*The opinions expressed are those of the author(s) and do not necessarily reflect the views of their employer, its clients, or Portfolio Media Inc., or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.*

[1] David Jones, "In 2024, the cybersecurity industry awaits more regulation — and enforcement," Cybersecurity Dive (January 31, 2024), https://www.cybersecuritydive.com/news/cyber-enforcement-regulation/706141/.

[2] "New rules to boost cybersecurity of the EU institutions enter into force," European Commission (January 8, 2024), https://ec.europa.eu/commission/presscorner/detail/en/IP_23_6782.

[3] "What is GDPR, the EU's new data protection law?," GDPR.EU (April 5, 2024), https://gdpr.eu/what-is-gdpr/.

[4] "Digital Operational Resilience Act (DORA)," European Insurance and Occupational Pensions Authority (April 5, 2024), https://www.eiopa.europa.eu/digital-operational-resilience-act-dora_en.

[5] "The Digital Services Act package," European Commission (April 5, 2024), https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package.

[6] "SEC Adopts Rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies," U.S. Securities and Exchange Commission (July 26, 2023), https://www.sec.gov/news/press-release/2023-139.

[7] "Cybersecurity Requirements for Financial Services Companies," New York State Department of Financial Services (April 5, 2024), https://www.dfs.ny.gov/system/files/documents/2023/03/23NYCRR500_0.pdf.

[8] "California Consumer Privacy Act (CCPA)," Sate of California Department of Justice (March 13, 2024), https://oag.ca.gov/privacy/ccpa.

[9] "Summary of the HIPAA Privacy Rule," U.S. Department of Health and Human Services (April 5, 2024), https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html.

[10] "CISO Redefined: Navigating C-suite Perceptions & Expectations," FTI Consulting (March 26, 2024), https://fticommunications.com/ciso-redefined-navigating-c-suite-perceptions-and-expectations/?topic_origin=ciso-communications-redefined.