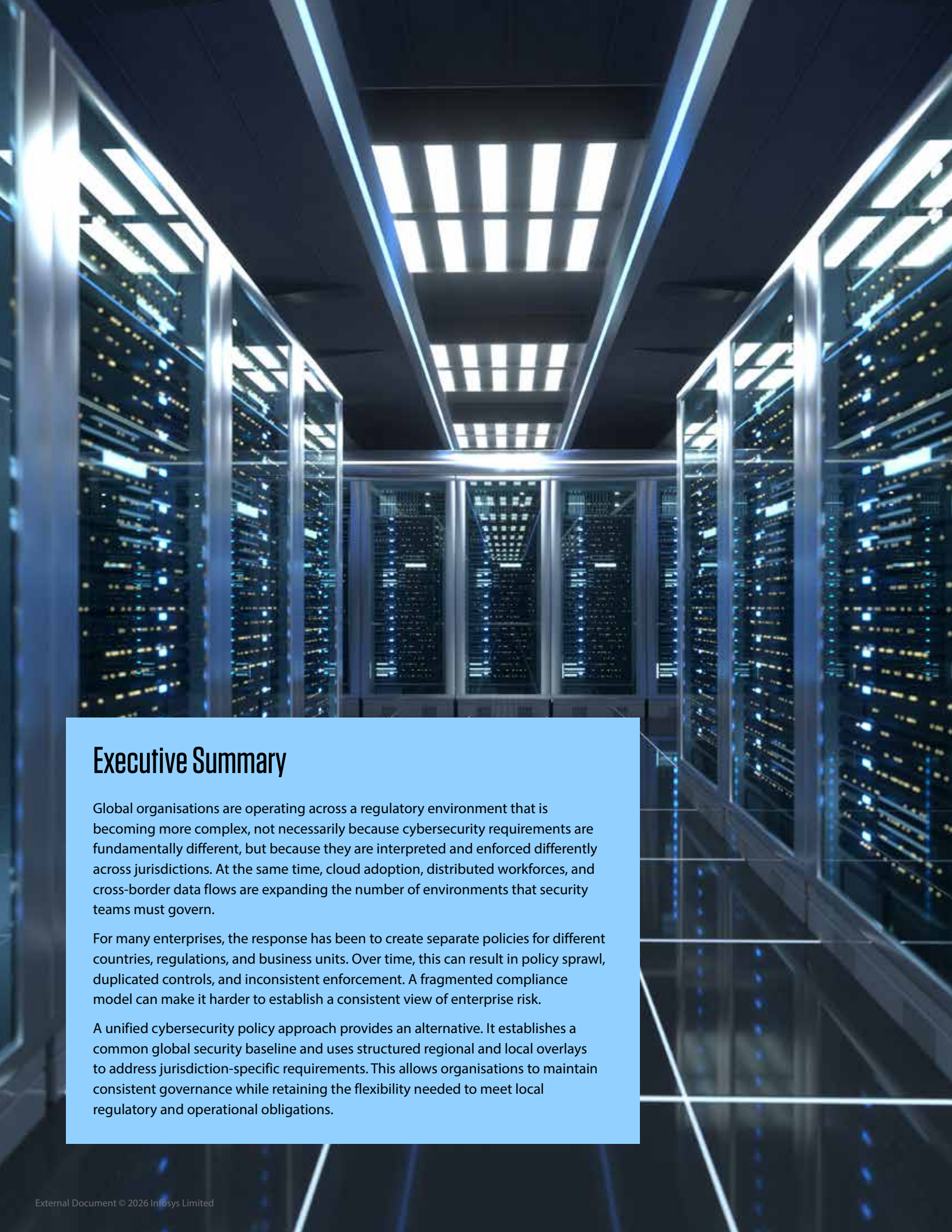
VIEW POINT



NAVIGATING GLOBAL COMPLIANCE: A UNIFIED CYBERSECURITY POLICY APPROACH

Infosys
Navigate your next



Executive Summary

Global organisations are operating across a regulatory environment that is becoming more complex, not necessarily because cybersecurity requirements are fundamentally different, but because they are interpreted and enforced differently across jurisdictions. At the same time, cloud adoption, distributed workforces, and cross-border data flows are expanding the number of environments that security teams must govern.

For many enterprises, the response has been to create separate policies for different countries, regulations, and business units. Over time, this can result in policy sprawl, duplicated controls, and inconsistent enforcement. A fragmented compliance model can make it harder to establish a consistent view of enterprise risk.

A unified cybersecurity policy approach provides an alternative. It establishes a common global security baseline and uses structured regional and local overlays to address jurisdiction-specific requirements. This allows organisations to maintain consistent governance while retaining the flexibility needed to meet local regulatory and operational obligations.

External Document © 2026 Infosys Limited

The Industry Problem: Fragmented Cybersecurity Compliance

The Global Compliance Landscape

Cybersecurity compliance has shifted from being a primarily regional obligation to a global operational priority. Regulators continue to introduce requirements covering data protection, cyber resilience, critical infrastructure defences, and third-party risk. While these regulations often share common security principles, their interpretation and enforcement can vary significantly across jurisdictions.

For organisations operating across multiple markets, this creates a practical challenge: how can security leaders maintain consistent enterprise-wide controls while responding to different regulatory expectations? This complexity is pushing enterprises toward implementing more cohesive, scalable approaches to cybersecurity governance.

The widespread adoption of cloud services, distributed workforces, and interconnected digital ecosystems has further amplified the threat landscape. Operating across multiple regulatory environments means organisations must balance different compliance expectations while preserving consistent security standards. This rising complexity underscores the need for unified cybersecurity policy frameworks that deliver both regulatory alignment and strong, resilient security across the entire global enterprise.

Background: The Structural Weakness of Region-Specific Policies

Historically, cybersecurity policies have often been created in response to specific regulatory or operational requirements. As organisations expanded into new markets, additional policies were introduced to address local obligations, often without being fully aligned with existing governance structures.

Over time, this can create policy sprawl. Different regions may interpret similar requirements differently, maintain overlapping controls or develop their own processes for demonstrating compliance. The result is not a documentation problem alone. Fragmented policies can create differences in how security controls are implemented, monitored, and enforced across the enterprise.

Meanwhile, the threat landscape has grown increasingly sophisticated. Modern cyber adversaries often focus on organisations with distributed, complex environments, taking advantage of the security gaps that arise from disjointed policy landscape and governance. This evolving risk environment has made it clear that organisations need a more unified and coordinated approach to cybersecurity policy management.

Why Conventional Compliance Models Fall Short

A region-by-region approach may appear practical because it allows local teams to respond directly to local requirements. However, it becomes difficult to scale when an organisation operates across multiple regulatory environments.

Legacy technology can make standardised control implementation difficult. Some environments may not support centralised identity management, logging, or automated compliance monitoring. Data residency and cross-border data-sharing requirements may also need local control execution.

Organisational factors add another layer of complexity. Regional teams accustomed to managing their own policies may view centralised governance as restrictive or poorly aligned with local operational realities.

Even when policies are formally standardised, differences in interpretation can produce inconsistent execution. Vulnerability remediation, access reviews and other control activities may therefore operate to different standards across business units.

External Document © 2026 Infosys Limited

Business and Operational Consequences

Fragmented cybersecurity compliance creates several enterprise-level consequences.

Duplicated controls and documentation increase the effort required to demonstrate compliance. Parallel policies make it harder to establish a single view of security posture. Differences in control implementation can also create gaps that are difficult to identify through enterprise-level reporting.

The impact also extends to audits and regulatory change. When requirements evolve, organisations may need to assess and update multiple policy environments rather than applying changes through a common governance framework.

A more scalable approach requires organisations to distinguish between what should remain consistent globally and what genuinely needs to vary by jurisdiction.

The Architectural Shift: Unified Cybersecurity Policy

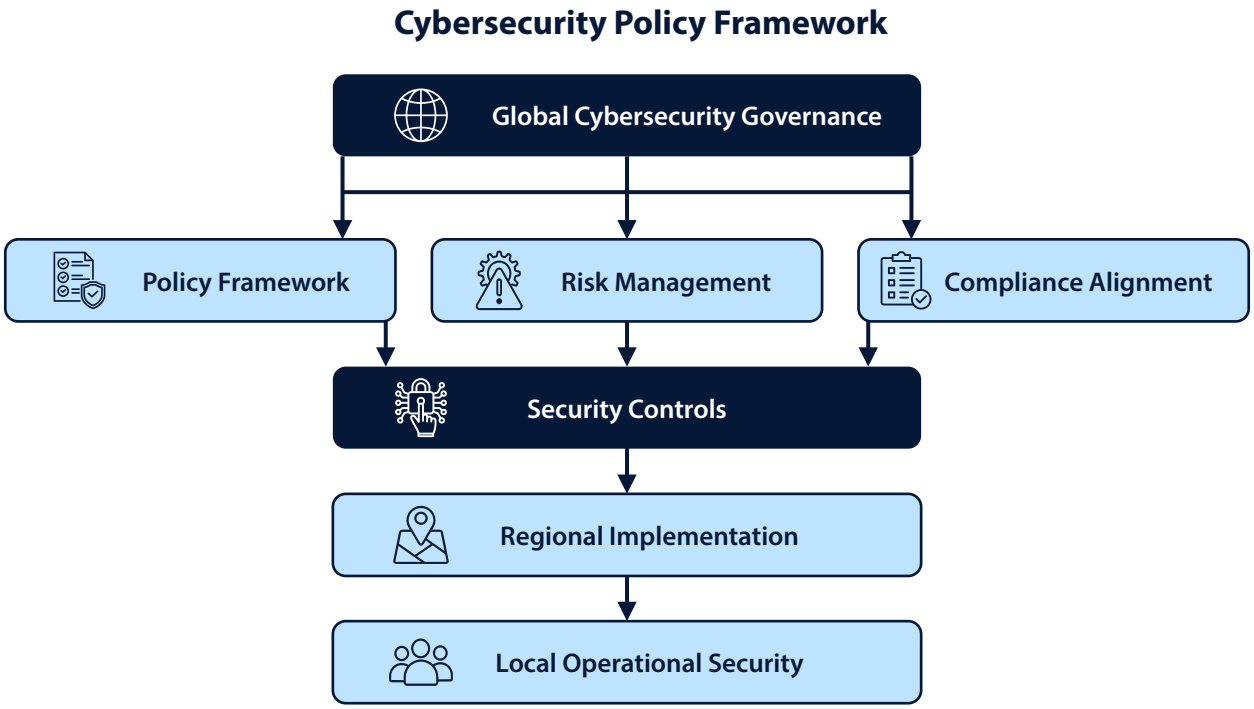


Figure 1: Unified Cybersecurity Policy Governance Model

A unified cybersecurity policy model establishes a common enterprise-wide security baseline while allowing regional and local requirements to be incorporated through structured policy overlays. Rather than maintaining independent policies for each geography or regulation, the model establishes a global baseline of security principles and controls, augmented by regional and local overlays where required.

At the centre is centralised governance, which defines enterprise-wide cybersecurity policies, control objectives, risk tolerance, and compliance alignment. This layer ensures that security intent, control design, and accountability remain consistent regardless of where systems, data, or users are located.

Beneath this layer, standardised security control frameworks translate policy intent into actionable and testable controls aligned with leading industry standards. These control sets act as the common foundation across business units and technology environments.

Regional and country-specific regulatory requirements are then incorporated as structured enhancements to the global baseline rather than being developed as independent policy sets, reducing duplication and inconsistency.

Finally, regional and local implementation layers adapt these controls to operational realities such as technology maturity, legal constraints, workforce capabilities, and third-party ecosystems. This creates a model in which global consistency and local regulatory flexibility can coexist.

External Document © 2026 Infosys Limited

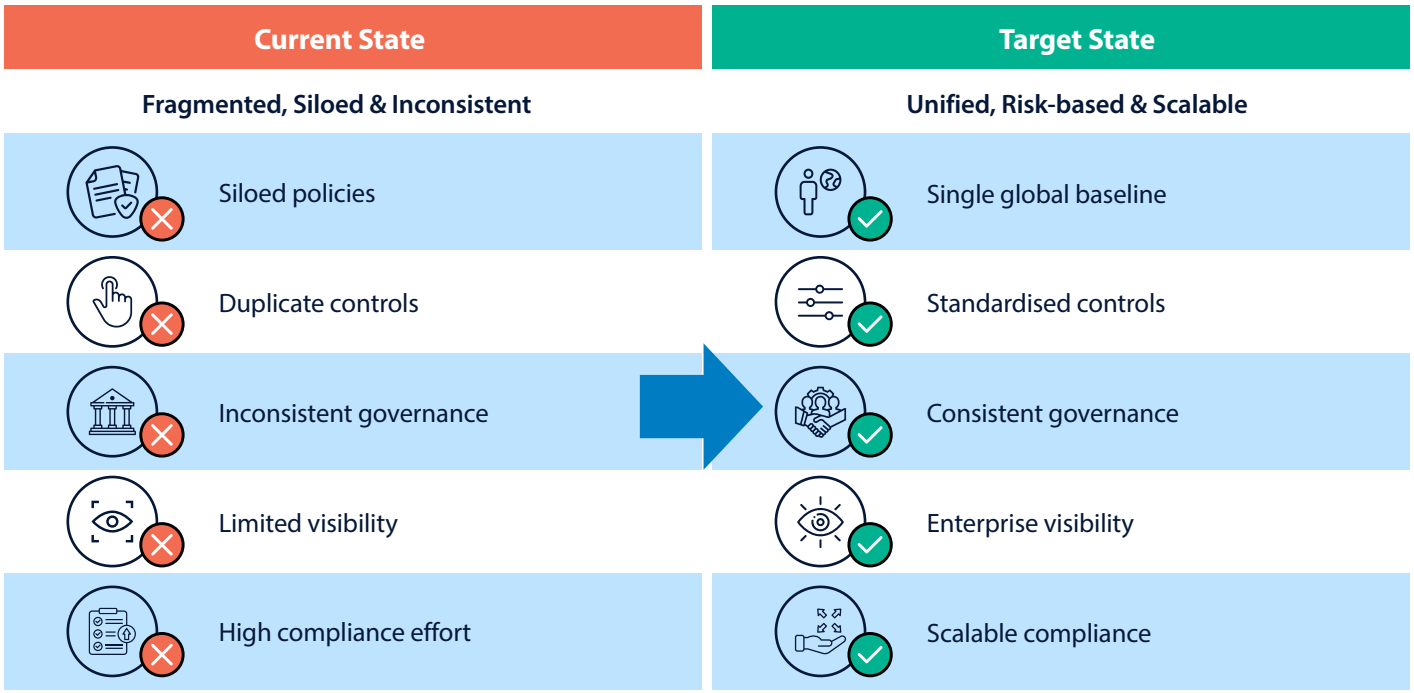
This model enables organisations to:

- Maintain a single version of policy truth and avoid parallel policy universes while still respecting local, legal, and regulatory requirements.
- Eliminate local reinvention, enabling consistent interpretation and adoption of cybersecurity policies across regions and business units.
- Accelerate audit and response cycles, providing seamless visibility and action from local environments through to the enterprise level.
- Reduce duplication of controls, documentation, and cost by demonstrating control consistency and reuse across regulatory and compliance obligations.
- Enable scalable compliance, allowing organisations to adapt efficiently as regulations evolve at enterprise, industry, and local levels.

Comparing the two models

The following visual contrasts the limitations of region-specific cybersecurity compliance models with the benefits of a unified, enterprise-wide approach.

Current State vs Target State



Implementation Realities

Implementing a unified policy framework is not simply a matter of publishing a global policy. Organisations must account for heterogeneous technology environments, legacy systems, regional platforms, and cloud services. Some jurisdictions may require sensitive data or security logs to remain within national boundaries, limiting the extent to which monitoring can be centralised.

Governance must therefore distinguish between policy consistency and implementation uniformity. The policy intent and control objectives can remain consistent while the way a control is executed may vary because of technology, legal, or operational constraints.

Regional ownership is equally important. A unified framework should define clear responsibilities across global, regional, and local teams, including exception management, escalation, and accountability.

External Document © 2026 Infosys Limited

Geographic Cybersecurity Compliance Landscape

Cybersecurity regulatory expectations and associated risks vary significantly across geographic regions, influencing how unified cybersecurity policies are implemented and governed. The following table provides a simplified overview of key regulatory environments and related cybersecurity risk considerations.

Region	Regulatory Environment	Key Cybersecurity Risk
North America	Mature regulatory frameworks with strong enforcement	Complex compliance requirements across federal and state levels
Europe	Strict data protection and cybersecurity regulations	High compliance obligations and strong privacy expectations
Asia-Pacific	Rapidly evolving cybersecurity regulations	Inconsistent regulatory maturity across countries
Middle East	Increasing national cybersecurity initiatives	Growing focus on critical infrastructure protection



External Document © 2026 Infosys Limited

Best Practices for Unified Cybersecurity Policy at Scale

When adopting a unified cybersecurity policy framework, organisations must address several important considerations to ensure effective governance and sustainable implementation.



Establish a Global Security Baseline.
Define minimum cybersecurity expectations across regions, business units, and technology environments. The baseline should reflect business objectives, risk appetite, and the organisation's regulatory obligations.



Map Regulations to Common Controls
Regulatory and industry requirements should be mapped against the enterprise baseline to identify common control expectations and genuine areas of regional variation.



Define Governance and Accountability.
Clearly establish policy ownership and decision rights across global, regional, and local teams. Exception management and escalation processes should be part of the governance model rather than handled informally.



Build in Risk-Based Flexibility.
A unified framework should not require every control to be implemented identically. Variation may be appropriate based on data sensitivity, business criticality, threat exposure, and local legal requirements.



Align Policy with Operational Reality.
Policies need to work with existing technology, processes, and workforce capabilities. Overly prescriptive requirements can create resistance or lead to inconsistent adoption.



Monitor, Report, and Continuously Improve.
Standardised metrics and reporting should provide an enterprise-level view of compliance and security posture. Regular policy reviews, regulatory horizon scanning, and risk assessments can help the framework adapt as requirements change.

For example, an Infosys client — a Swiss global financial services company — achieved a 20 percent cost reduction through efficiency improvements by aligning its compliance program to ISO 27001 and ISAE 3402 requirements.

External Document © 2026 Infosys Limited



Overall Approach to Unified Cybersecurity Policy Adoption

Key Considerations for a Unified Approach

Global Baseline	Regulatory Mapping	Governance & Roles	Traceability & Visibility	Monitoring & Improvement
Establish a common security baseline applicable across all regions.	Align global policy with regional regulations and industry standards.	Define clear roles, responsibilities and accountability across the organization.	Ensure end-to-end traceability from policy to controls to regulations.	Continuously monitor compliance and improve through insights and feedback.

Organisations should begin by establishing a common enterprise security baseline aligned with business objectives, risk appetite, and regulatory expectations. This baseline provides the foundation for consistent cybersecurity governance across geographies.

Regulatory and industry requirements should then be consolidated and mapped to this baseline to identify common control expectations and areas requiring regional enhancement. This structured mapping enables rationalisation of controls, reduces redundancy, and improves consistency in compliance management.

Where jurisdiction-specific obligations apply, structured policy overlays can be introduced without modifying the core framework. Implementation should be supported by standardised processes, enabling technologies, and measurable metrics to ensure effective execution. Continuous governance activities, including policy and controls compliance reviews, regulatory horizon scanning, and risk assessments, help ensure the framework remains resilient as regulatory and threat landscapes evolve.

External Document © 2026 Infosys Limited

Interlocks Between Industry Practices and Regulations

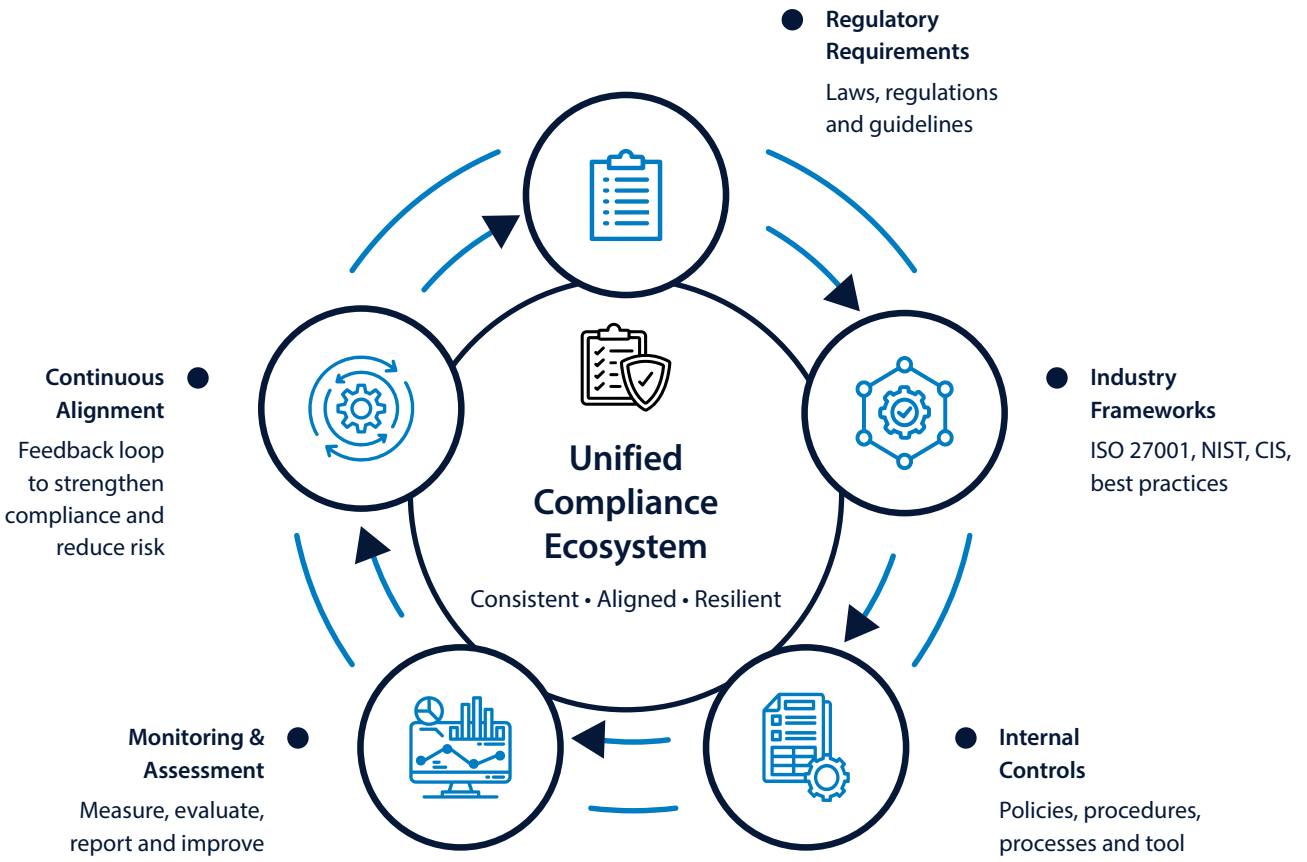
Industry standards can provide a common reference point when organisations need to translate different regulatory requirements into consistent controls.

Frameworks such as ISO 27001 and the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) can support this process by providing established control and risk-management principles.

Rather than treating every regulation as a separate compliance exercise, organisations can use common frameworks to identify areas of overlap and establish reusable controls. This interconnected approach allows organisations to streamline compliance efforts. A single, well-structured control framework can satisfy multiple regulatory mandates, reduce duplication, and enable more efficient policy implementation. It also strengthens communication with regulators and auditors by demonstrating a clear, risk-based governance model rooted in recognised industry best practices.

As regulatory bodies increasingly incorporate or reference established cybersecurity standards, aligning internal policies with these frameworks becomes even more valuable. It simplifies regulatory mapping, improves the consistency of compliance assessments across regions, and supports a unified cybersecurity policy framework that can flexibly absorb new or changing requirements. Ultimately, this alignment helps organisations maintain strong, consistent security practices while meeting diverse regulatory expectations across global operations.

Interlock Between Regulations & Practices



External Document © 2026 Infosys Limited

Enterprise Enablement and Operating Capabilities

Sustaining a unified cybersecurity policy framework requires strong governance structures, regulatory insight, and scalable operating capabilities. Effective enablement involves rationalising fragmented policy environments into cohesive frameworks that align regulatory obligations with standardised security controls.

A unified cybersecurity policy framework requires more than policy documentation. It needs scalable operating capabilities that support governance, regulatory insight, control implementation, and continuous monitoring.

Clear operating models should define ownership, oversight, and escalation mechanisms across global and regional teams. Governance platforms, and automated compliance reporting and monitoring capabilities can provide greater visibility into security posture and compliance status.

Ongoing maturity assessments and stakeholder alignment can then help embed the framework into day-to-day operations.

Infosys Cyber Next provides an example of how this model can be operationalised. Its platform-powered governance, risk and compliance capabilities span quantified cyber risk management, security awareness, and enterprise security architecture management, with alignment to global standards such as the NIST Cybersecurity Framework and ISO 27001. Delivered through Cyber Defense Centers across the US, Europe and APAC, the model combines common governance and standards with geographically distributed capabilities.

Conclusion

Global cybersecurity compliance is becoming too complex to manage effectively through an expanding collection of region-specific policies. A unified cybersecurity policy approach provides a more scalable alternative: one enterprise-wide security baseline, supported by common controls and structured regional overlays where local requirements demand them.

The objective is not to eliminate regulatory differences. It is to manage those differences within a consistent governance model. For organisations operating across multiple markets, this shift can reduce duplication, improve traceability, and provide stronger visibility into enterprise-wide security risk while retaining the flexibility needed to meet local obligations.

The next step for security leaders is therefore to assess where fragmented policies exist today, identify common control requirements, and establish a roadmap towards a unified policy and governance model.

External Document © 2026 Infosys Limited

References

- *European Union Agency for Cybersecurity. (2025). ENISA threat landscape 2025.* *https://www.enisa.europa.eu/publications/enisa-threat-landscape-2025*
- *Organisation for Economic Co-operation and Development. (2026). Towards international coherence of cybersecurity regulations (OECD Digital Economy Papers No. 384). OECD Publishing.* *https://doi.org/10.1787/bd1f199a-en*
- *World Economic Forum. (2026). Global cybersecurity outlook 2026.* *https://www.weforum.org/publications/global-cybersecurity-outlook-2026/*
- *World Economic Forum. Global Cybersecurity Outlook 2025.* *https://www.weforum.org/publications/global-cybersecurity-outlook-2025/in-full/executive-summary-4e44b16c32*
- *Infosys Cyber Next* *https://www.infosys.com/services/cyber-security/offerings/platform-powered-services.html*

External Document © 2026 Infosys Limited

For more information, contact askus@infosys.com

© 2026 Infosys Limited, Bengaluru, India. All Rights Reserved. Infosys believes the information in this document is accurate as of its publication date; such information is subject to change without notice. Infosys acknowledges the proprietary rights of other companies to the trademarks, product names and such other intellectual property rights mentioned in this document. Except as expressly permitted, neither this documentation nor any part of it may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, printing, photocopying, recording or otherwise, without the prior permission of Infosys Limited and / or any named intellectual property rights holders under this document.