iapp

Organizational Digital Governance Report 2024

Table of contents

What's inside?

From digital entropy to digital responsibility

It is within our instincts and skills as a profession to ensure entropy does not take hold.

Entropy is a scientific term commonly associated with a state of disorder and uncertainty. One characteristic of entropy is that, according to theory, it increases over time. Unmanaged or unchecked, entropy begets more entropy.

As new technologies are developed, integrated and deployed across our societies, the impacts are far-reaching, transformative and, at times, destabilizing. Along with creating great opportunities and new risks, they can upend the status quo, bringing disorder to carefully crafted governance and regulatory mechanisms often designed for the predigital era. New regulatory, ethical and organizational initiatives aim to ensure such technologies are used responsibly and safely. In short, these initiatives seek to empower our ability to push back against the steady increase of entropy as technological innovation moves forward. Put simply, regulatory frameworks often provide the structures upon which we manage the complexity of new technology.

Understanding and navigating the overlaps, gaps and even conflicts between these regulatory domains is complex work for businesses and organizations.

However, regulatory architectures can also add a perceived sense of disorder, creating conflicting, overlapping and shifting compliance requirements. Laws and policies on data protection and privacy, cybersecurity, consumer protection, competition, content moderation, online safety, artificial intelligence, and intellectual property all exist in an increasingly complex digital regulatory environment. For example, as part of its Digital Strategy, the EU has built a broad framework for digital governance — with the EU General Data Protection Regulation, Digital Services Act, Digital Markets Act, Data Governance Act, Data Act, AI Act, European Health Data Space, eIDAs regulation and NIS2 Directive all contributing to a growing body of standards for the digital market to follow. But the EU is not alone. Whether due to the "Brussels effect" or otherwise, regulations pertaining to the governance of digital technologies are being promulgated and are proliferating worldwide. Understanding and navigating the overlaps, gaps and even conflicts between these regulatory domains is complex work for businesses and organizations. It is harder still to coordinate and operationalize a response. And it is even harder to deliver that response. Failing to do so can be hugely consequential to an organization's efficacy, integrity or even existence. This is digital entropy.

In science, the directional arrow of entropy is immutable. It is inexorable. Science's entropy is always increasing. Digital entropy is, however, capable of mitigation and management. We can bend the arc of digital entropy back toward order. We can tame the complexity of technological innovation and regulatory response.

But how?

Designing and implementing effective structural responses to the complexity of our digital regulatory world is ascending as a strategic priority within organizations. Since January, the IAPP has been researching the extent to which organizations currently or intend to structure their resources and decision-making to respond to digital governance. We have done so through a series of interviews with more than 20 senior leaders at some of the world's foremost digital technology-enabled organizations. We asked whether their organizations defined digital governance, how they defined it and about the roles of various internal functions and external resources in coordinating their organization's response to digital governance.

Of course, there is more to an organization's response to digital entropy than just its internal organizational structure. Communications, processes, documentation, other tools, staff training and broader enterprise risk management are all formative factors in whether and how an organization delivers on its response to digital entropy. That said, triaging and deciding on all these factors does not take place in a vacuum. It takes place within, depends upon and even reflects the design and efficacy of the organization's internal structure.

Our research brings some clarity to the complexity of our current digital policy environment. Perhaps more importantly, it highlights the critical need for professionals — with appropriate tools and resources — to respond to the challenge of this moment. It is, in many ways, a call to action for all of us.

J. Trevor Hughes, CIPP
President and CEO, IAPP

Joe Jones
Director of Research and Insights, IAPP

Executive summary

The alphabet soup of digital governance regulation is complex and continually evolving.

The importance of organizational digital governance is driven by a combination of factors. Chief among them is how the acceleration, ubiquity and integration of new digital technologies are met with new regulatory, ethical and organizational initiatives that aim to ensure such technologies are used safely, responsibly and in compliance with applicable requirements.

The alphabet soup of digital governance regulation is complex and continually evolving. Organizations are leveraging and evolving existing governance structures to respond. Many are doing so with long-standing decentralized organizational approaches to governance that have yet to be meaningfully, let alone effectively, cohered and coordinated.

Research approach

Senior decision-makers are seeking to understand how organizations are defining and implementing their internal structures. In the absence of publicly available information on organizations' internal governance structures, the IAPP sought to interview senior leaders across various organizations to understand:

1. The extent to which digital governance has been defined.
2. The domains in scope for digital governance, responsibilities for those domains and reporting lines.
3. The functions, structures, processes and people currently in place or likely to be established or appointed to support digital governance.
4. The extent to which tooling is available to support a transition to a more effective digital governance model.

Interviews were conducted with more than 20 senior decision-makers who lead their organization's work on various aspects of digital governance. This includes insights from some relevant regulators. Given the focus on large multinationals, our insights are skewed toward organizations that are likely more mature in their approaches to organizational governance.

This report seeks to show some of the findings from those interviews, including by building out illustrative organizational charts that convey the variety, nascency and direction of travel in how organizations approach the transition to more cohered and coordinated organizational digital governance.

The insights and models presented are intended to facilitate discussion. They are not indicative of any one organization or intended to recommend any particular model to organizations. An important reflection from the interviews is how formative and consequential an individual organization's culture and footprint is to their chosen model. Every organization occupies a unique place in the wider environment. Different business models, digital technology applications, risk exposures and appetites, and resources all impact how organizations consider the design and implementation of their organizational digital governance.

Ultimately, many of the interviewed organizations acknowledged more work is needed to implement a coherent, efficient and effective digital governance program. Interviewees identified building a sustainable digital governance approach will involve careful consideration of how domains and disciplines can be bridged, as well as how communications, decision-making and accountability will flow up, down and across the organization. Solely addressing the issue by adding resources, whether that is additional staff, budget or even committees, is unlikely to solve the challenge.

We welcome feedback on how your organization intends to cohere and coordinate its response to the increasingly complex landscape of digital governance.

Saz Kanthasamy
Principal Researcher, Privacy Management, IAPP

What is organizational digital governance?

Many organizations struggle with whether and how to define and cohere digital governance.

Part of that struggle is due to the changing macroenvironment and the number and variety of subject matter domains within digital governance.

By organizational digital governance, we refer to the structures and frameworks that establish roles, responsibilities and accountability for an organization's approach to the sociotechnical, strategic and regulatory domains associated with digital technology.

For some organizations — especially digital technology companies — digital governance is the vast majority of or is synonymous with enterprise risk governance. For others, digital governance is much more discrete as a part of broader enterprise risk governance efforts, even if it is not yet defined.

Broadly speaking, digital governance encompasses any combination of privacy and data protection, AI governance, cybersecurity, content moderation, online safety, platform liability, digital accessibility, data governance, and ethics. It can also include governance needs associated with copyright, trade, law enforcement and national security, competition, third-party management, and civil rights as they intersect with a company's development, use or deployment of digital goods and services.

Responsibilities for digital governance can exist across different lines of defense within an organization to a greater or lesser extent.

First line: Front-line teams

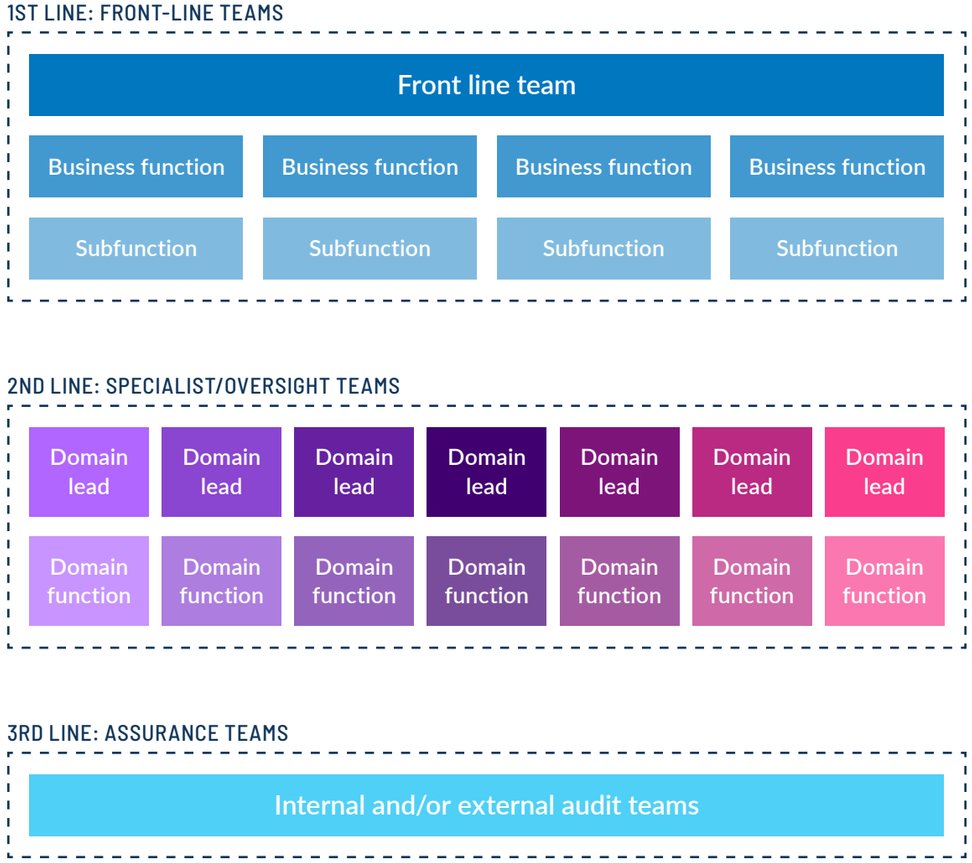
Teams on the front line own and manage risks and likely work within various business functions like the business and product teams. They are likely responsible for managing operational risks by designing and implementing appropriate mitigating controls.

Second line: Specialist/oversight teams

This primarily consists of teams that oversee or provide subject-matter expertise in governance, risk management and compliance, e.g., risk management, privacy and information security. They may be responsible for helping the first-line teams build mitigating controls, monitoring their effectiveness, and developing policies and procedures for risk management.

Third line: Assurance teams

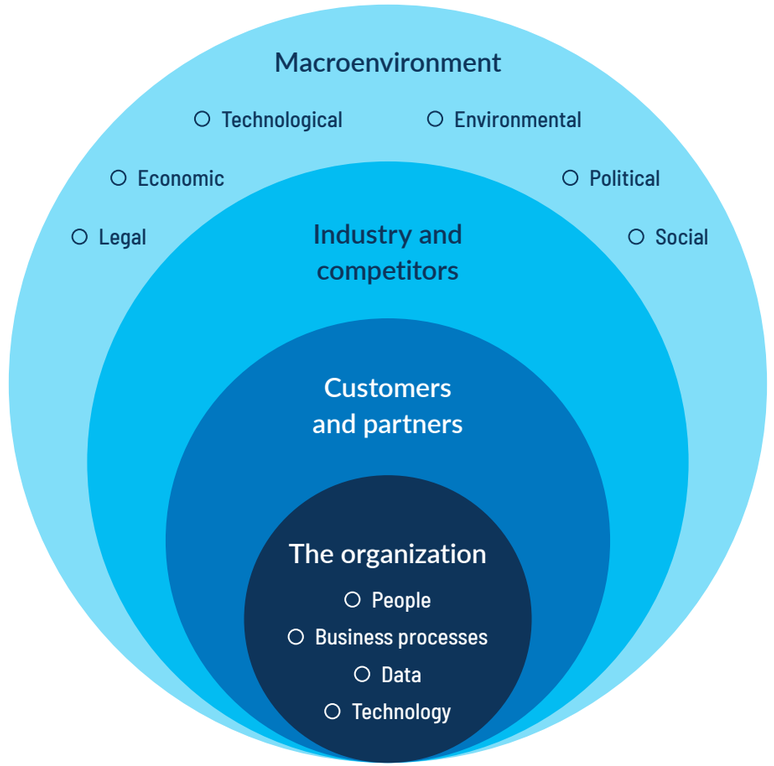
Internal audit teams provide independent assurance to identify whether teams in the first two lines are operating effectively. Responsibilities likely include providing independent reporting to management.



Contexts, drivers and levers

The importance of organizational digital governance is driven by a combination of factors.

The graphic below outlines the internal and external factors organizations should consider when defining digital governance for their organization, building out a digital governance framework and deploying digital governance controls.



Macroenvironment: The political, economic, social, technological, environmental and legal factors driving digital governance adoption.

- **Political:** The impact of the broader domestic and international political environments and government interventions require navigation, anticipation and response. Examples include increased regulation or deregulation, evolving regulatory intervention, political reform and stability.

- **Economic:** Factors such as economic growth, interest rate fluctuations, inflation, wage rates and cost of living all impact digitization and digital governance, as well as organizational decision-making.

- **Social:** Cultural norms and expectations, consumer attitudes toward digital services and organizations, as well as shifting demographics all have the potential to impact an organization's digital strategy and compliance approach.

- **Technological:** These factors are among the most likely to have a direct impact on an organization's need to enhance its digital strategy. Factors from the rapid proliferation of AI technologies through to increased automation and rate of technological change all impact the way organizations produce and deliver goods and services.

- **Environmental:** Climate change and global warming are increasingly driving organizations to consider sustainable practices. Efficient and ethical sourcing and supply chain intelligence are likely to go hand in hand with digital governance strategies.

- **Legal:** Continuous evolution in the legal landscape regulating digital governance domains, in part due to the rapid development of digital technologies, is likely to require a change in how organizations address digital governance. The introduction of interconnected, overlapping and even conflicting regulatory domains within and across borders accelerates and poses challenges for digital governance.

Industry: Across almost all industries, organizations are intensely competing with their rivals to attract customers and deliver on business objectives. The extent to which trust in digital goods and services is a market differentiator within the industry sector impacts resourcing and the public-facing nature of roles and responsibilities.

Customers: Customer preferences, including the priority placed on trustworthiness in relation to price, quality and other factors, are likely to influence governance structure and resourcing.

Organizations: Investors, products and services, and delivery models are likely to impact, and be impacted by, digital governance. The digital governance strategy may need to consider the role of third parties, both in supporting the organization's approach to digital governance and conducting assurance and monitoring over the design and operating effectives of digital governance controls.

An organization's approach to governance, risk and compliance will form the foundation of how it delivers on its digital governance approach. The following elements are likely to be key:

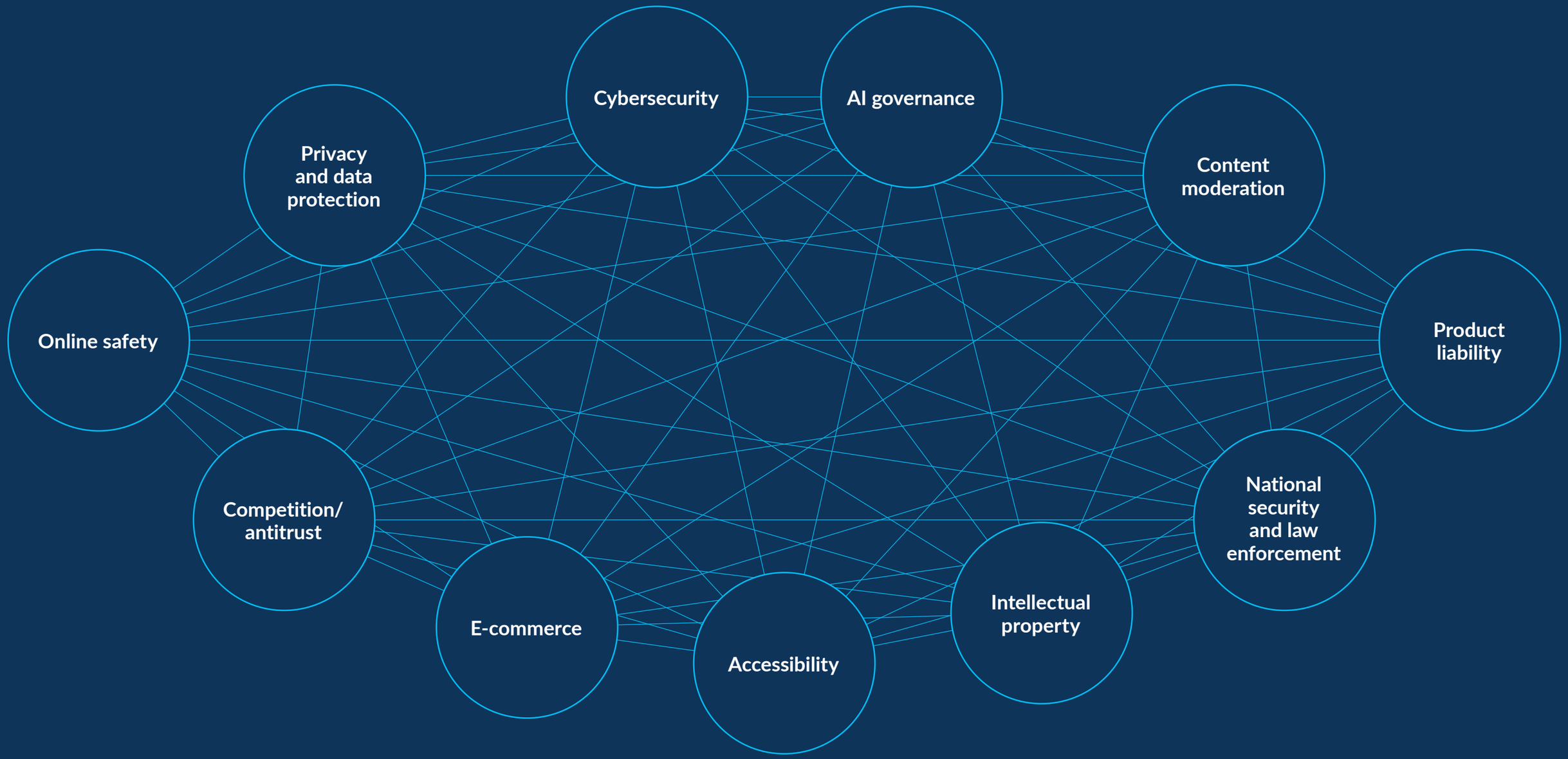
→ **People:** The resources, competencies, skills, culture, capability requirements and performance expectations for the organization to deliver on its approach to digital governance.

→ **Business processes:** The business and functional processes that enable the organization to deliver its products and services. Digital coherence among and within these processes is likely to play a key role in the successful deployment of digital governance. This includes understanding digital touchpoints and coordinating risk management through a single digital risk assessment that covers topics from privacy impact assessments to algorithm impact assessments and conformity assessments.

→ **Data:** Data is at the core of many organizations' delivery models, helping to make informed decisions, build evidence-based strategy and identify opportunities. Organizations can use their digital governance approaches to continuously and effectively balance competing forces between treating data as a liability and an asset.

→ **Technology:** Technology includes the applications, services and infrastructure used to deliver products and services. Digital governance technologies are also likely to play a key role, with single solutions that can integrate requirements across multiple compliance domains potentially able to deliver efficiencies over multiple disconnected platforms.

The matrix of digital governance domains



Responding to regulation

A significant accelerant for digital governance work is the proliferation of regulation.

The advent of new laws and policies, in combination with the application of long-standing regulations, has created a complex matrix of compliance obligations and risks for organizations. The risks associated with receiving a fine, being ordered to change business practices and experiencing broader reputational harm as a result of noncompliance are forcing functions on whether and how organizations categorize, prioritize and respond to digital governance. In the EU alone, the web of regulatory compliance obligations imposed by the GDPR, DSA, DMA, Data Act, NIS2 and, of course, the recently adopted AI Act perfectly illustrates the developing state of broader digital governance.

An increasing regulatory risk profile, as we see today, is resulting in the following trends within many organizations:

→ Design of governance processes, personnel and documentation that reflects mandated regulatory requirements, such as GDPR data protection officers and EU AI Act fundamental rights impact assessments.

→ Elevation of digital governance issues to more senior levels, including as a result of mandatory regulatory requirements.

→ Empowerment of legal and compliance functions and leadership.

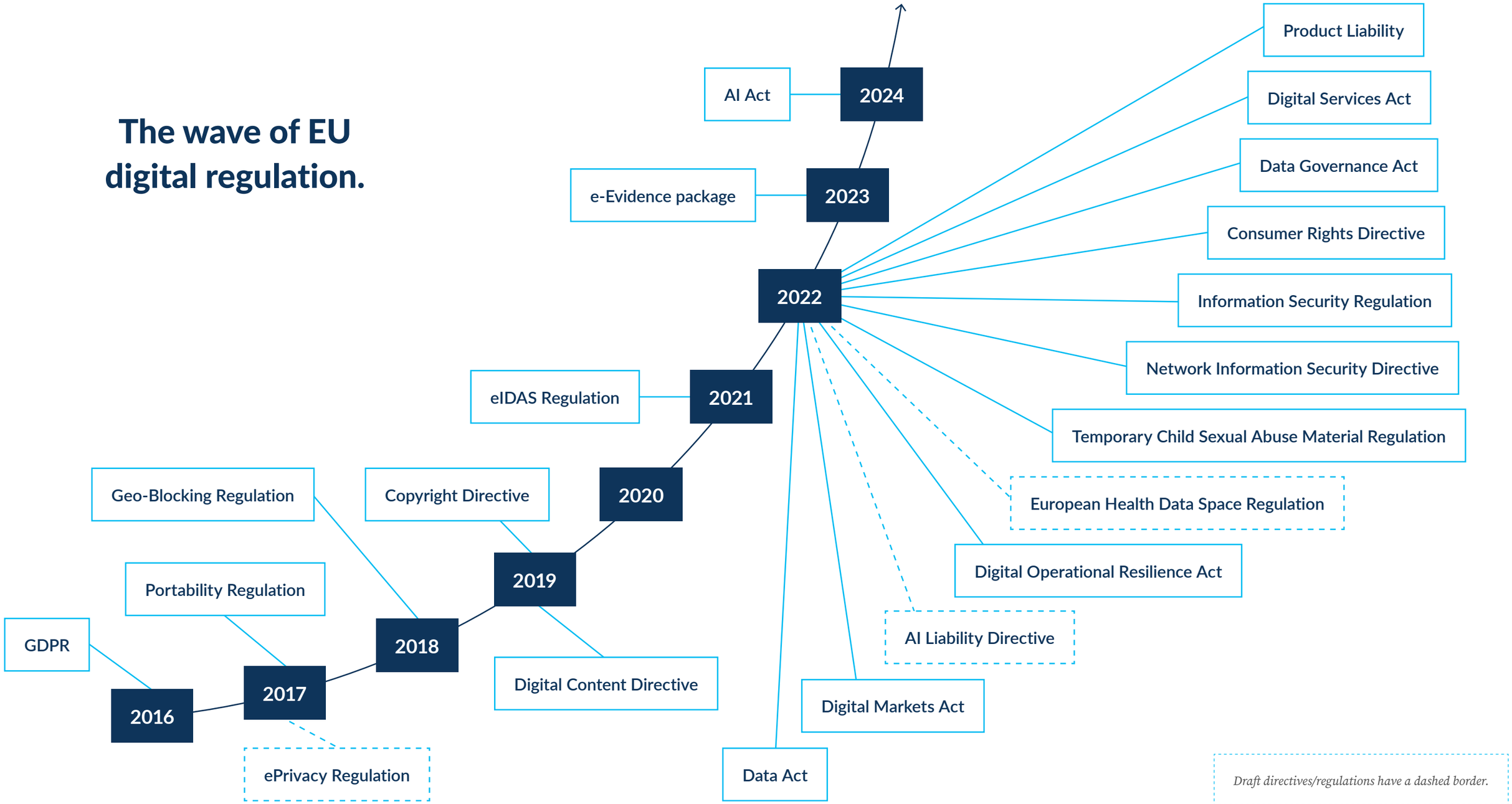
→ Investment in governance tooling to help business and product functions at the first line of defense.

→ Expansion of the scope, mandates and targets of existing compliance functions, in particular committees and mechanisms like risk assessments.

→ Incorporation of compliance risks into broader enterprise risk management.

But, as many respondents emphasized, regulatory compliance alone is not enough to build an effective approach to governance. If all digital governance professionals and functions did was consider and respond to regulations, enforcement decisions and court cases, they would miss the rest of the broader contexts, drivers and levers for digital governance, including more strategic objectives and opportunities associated with the utilization of technology and data.

The wave of EU digital regulation.



Draft directives/regulations have a dashed border.

C-suite responsibility: Arise, the chief ___ officer

Digital governance is expanding the role and responsibilities of the C-suite.

The perceived magnitude of regulatory compliance risks has long driven, and continues to drive, how some organizations designate responsibility and accountability at the C-suite level. General and chief legal and/or compliance counsels were the early designees. Thereafter, chief privacy officers, chief information security officers, chief technology officers and chief data officers all acquired prominent stakes. Today, organizations are considering whether and how to empower and expand the remits of existing C-suite members and/or the appointment of new C-suite members with responsibilities for digital governance writ large or for specific subdomains, e.g., the recruitment of chief AI governance officers.

One trend taking root is the expansion and greater empowerment of the role of the CPO. Some of this extends to include responsibility for other digital governance subdomains. For example, many CPOs have acquired responsibility for AI governance. The IAPP-EY Professionalizing Organizational AI Governance Report found 63% of organizations have tasked their privacy functions with AI governance responsibility. In some cases, the extension is even broader to include digital safety and ethics. These are logical extensions in many ways, given the disciplinary, regulatory and governance overlaps. This trend can be observed through the changing job titles in the market, with many additional descriptors tagged on to CPO titles over the past year.

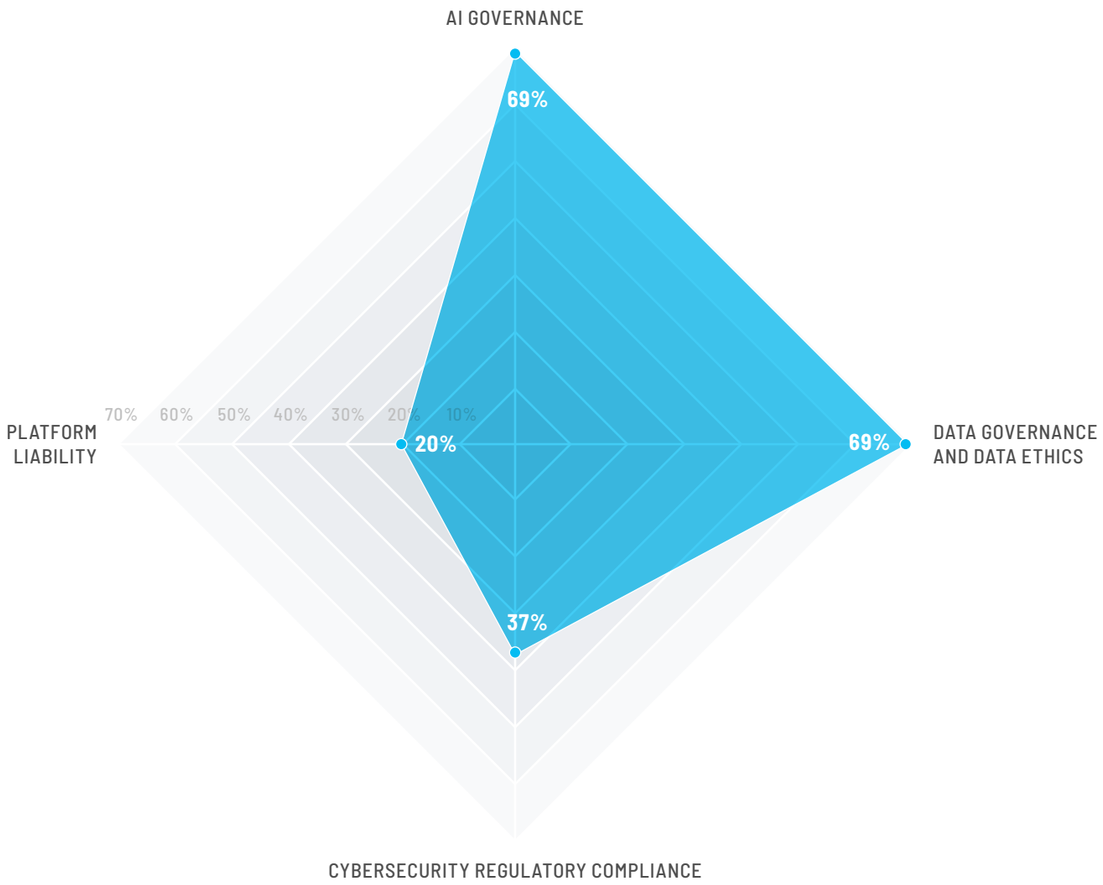
Even beyond the domains of privacy and AI governance, some companies have started to vest C-suite responsibility and accountability for broader digital governance domains.

Even beyond the domains of privacy and AI governance, some companies have started to vest C-suite responsibility and accountability for broader digital governance domains, especially those with ethics, trust or safety components, in the augmented CPO role. This has been the case even when organizations have not reformed other structures, such that individual domain functions remain disconnected at other levels in the organization.

In our engagement, the above trends have also taken place to a lesser extent when the CPO is also general counsel, chief legal officer or chief compliance officer, a combination that exists for many organizations.

Another emerging trend is combining traditionally regulatory responsive roles, such as the CPO, with roles and responsibilities more focused on strategic business objectives, such as data and digital transformation and utilization; broader environmental, social and corporate governance; and corporate resilience. At present, this trend is less visible in public-facing job title changes, such as the chief of digital strategy and governance officer.

The expanding remit for CPOs



Statistics gathered from the 2024 IAPP Governance Survey. More statistics and insights from the survey will be published later this year.

Existing C-suite leaders of specific domains are seeing their personal remits expanded and elevated.

For example, 69% of chief privacy officers surveyed have acquired additional responsibility for AI governance, while 69% are responsible for data governance and data ethics, 37% for cybersecurity regulatory compliance, and 20% for platform liability.

This trend continues at a team level, with over 80% of privacy teams gaining responsibilities that extend beyond privacy. At 55%, more than one in two privacy professionals works in functions with AI governance responsibilities. At 58%, more than one in two privacy pros has picked up data governance and data ethics. At 32%, almost one in three covers cybersecurity regulatory compliance. At 19%, almost one in five has platform liability responsibilities.

Roles with digital governance overlap

→ **CPO:** The CPO is responsible and accountable for an organizations' privacy compliance, management and strategy. Given this role's experience with establishing and cohering privacy compliance structures, data flows and information governance more generally, CPOs are targeted by the C-suite as a natural lead for digital governance efforts.

→ **CISO:** The CISO is tasked with leading the organization's approach to cybersecurity. Given this role's broad remit across the organization, CISOs likely play a key role in an organization's robust response to digital governance challenges.

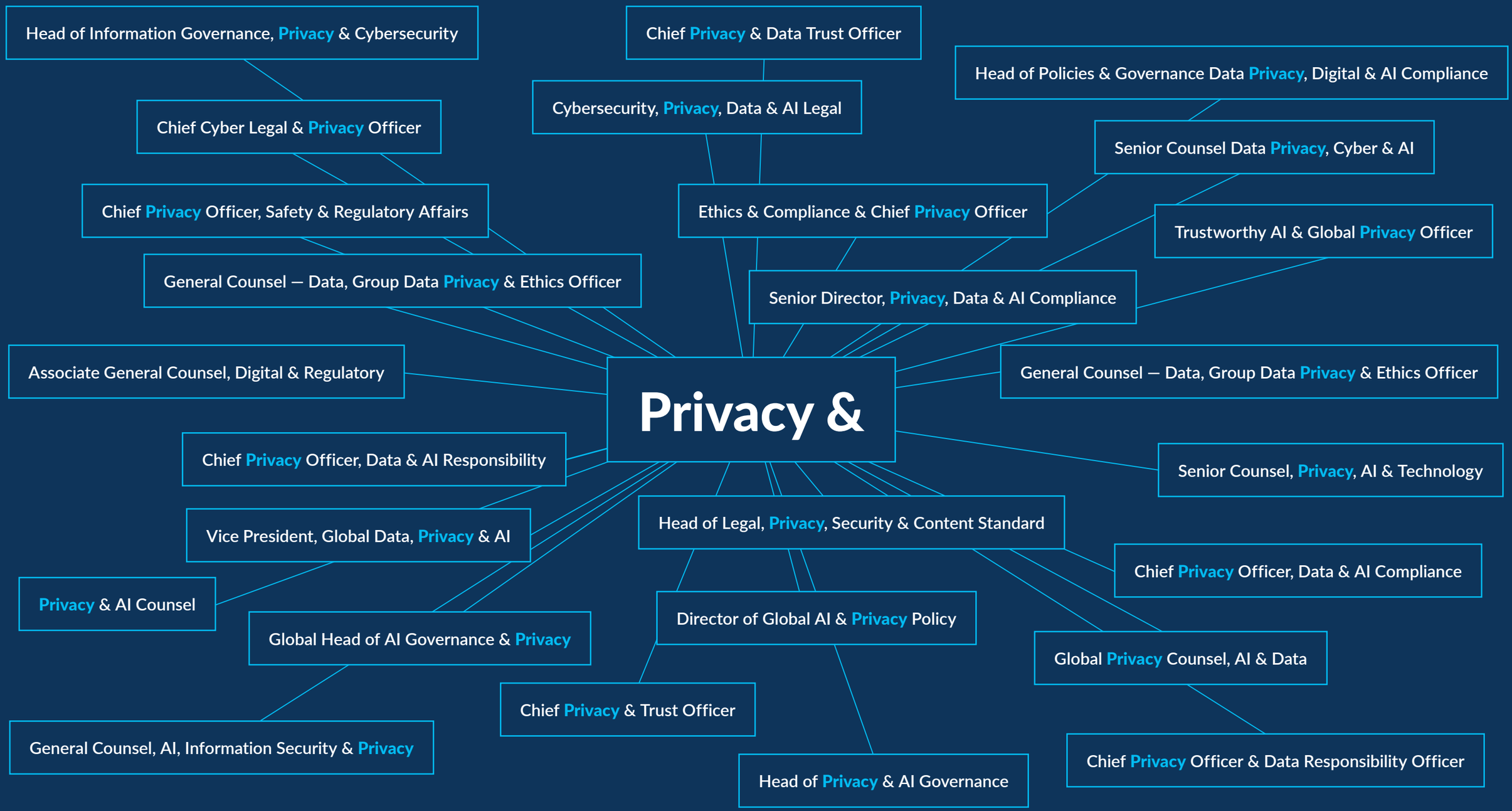
→ **Chief technology officer and/or chief information officer:** This role leads the organization's internal and/or external vision, resources, and strategies for technology development and utilization. An organization's technology strategy will likely be a key component of the extent to which it needs to create a digital governance strategy.

→ **Chief legal officer:** This role is accountable and responsible for an organization's legal affairs, such as regulatory compliance and contractual relationships. The chief legal officer plays a key role in supporting an organization's approach to responding to digital governance regulation and navigating its relationships with third parties.

→ **Chief data officer:** This role oversees data management-related functions within an organization. Data and the process of drawing valuable insights from that data likely form a key part of the maturity of an organization's approach to digital governance.

→ **Chief compliance officer:** The chief compliance officer oversees the organization's approach to managing regulatory compliance issues. This person's remit likely spans across multiple compliance domains and plays a key role in coordinating and cohering across in-scope digital governance domains.

→ **Chief risk officer:** This role is accountable for the organization's risk-management approach regarding both internal and external risks. They likely play a key role in the coordination and coherence of digital risks within digital governance models.


Head of Information Governance, Privacy & Cybersecurity
Chief Privacy & Data Trust Officer
Head of Policies & Governance Data Privacy, Digital & AI Compliance
Chief Cyber Legal & Privacy Officer
Cybersecurity, Privacy, Data & AI Legal
Senior Counsel Data Privacy, Cyber & AI
Chief Privacy Officer, Safety & Regulatory Affairs
Ethics & Compliance & Chief Privacy Officer
Trustworthy AI & Global Privacy Officer
General Counsel — Data, Group Data Privacy & Ethics Officer
Senior Director, Privacy, Data & AI Compliance
Associate General Counsel, Digital & Regulatory
General Counsel — Data, Group Data Privacy & Ethics Officer
Privacy &
Chief Privacy Officer, Data & AI Responsibility
Senior Counsel, Privacy, AI & Technology
Vice President, Global Data, Privacy & AI
Head of Legal, Privacy, Security & Content Standard
Chief Privacy Officer, Data & AI Compliance
Privacy & AI Counsel
Director of Global AI & Privacy Policy
Global Head of AI Governance & Privacy
Global Privacy Counsel, AI & Data
Chief Privacy & Trust Officer
General Counsel, AI, Information Security & Privacy
Chief Privacy Officer & Data Responsibility Officer
Head of Privacy & AI Governance

Analog governance

Organizational governance has been expanding and evolving organically in response to the proliferation of technology.

An analog model for an organization seeks to implement digital governance within and through individual subdomains without a defined or cohered approach to digital governance.

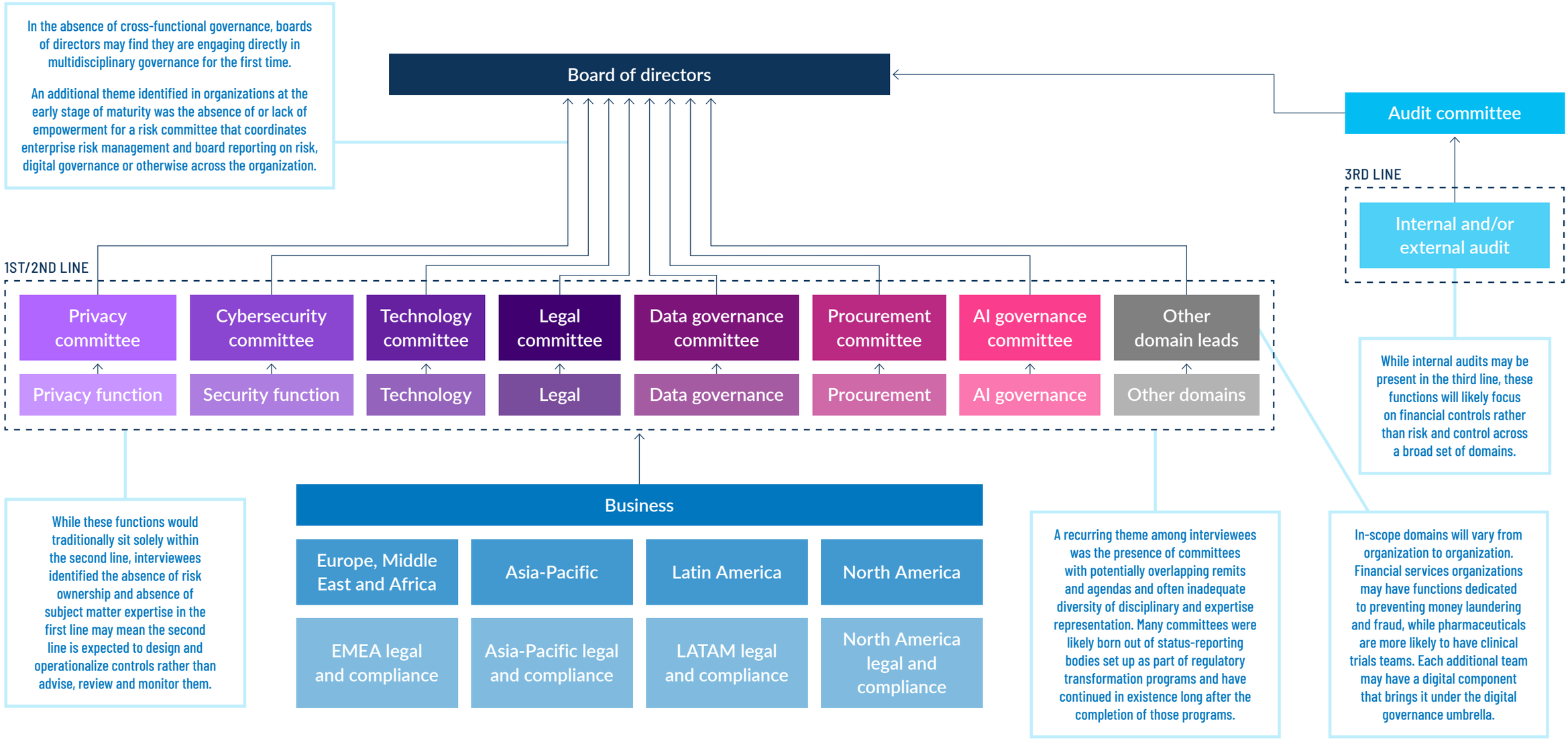
Most senior leaders interviewed indicated their organizations are early in their thinking and work to design and implement a digital governance framework. That is not to say those organizations are not putting digital governance into action; rather, they are doing so through and on top of existing structures that have largely not been coordinated by or cohered to a digital governance program. We have termed this analog governance.

Challenges to overcome in building and maturing digital governance approaches include:

- → A lack of maturity among the various second-line functions.
- → A lack of awareness, accountability and/or commitment by the first line of defense for risks.
- → An expectation by the first line and the broader organization that the second line will design and operationalize controls, impacting its ability to test and monitor those controls independently.

The organogram on the next page shows a high-level example organizational structure for digital governance. Committees have likely been stood up in direct response to regulatory and policy developments, with a remit to oversee operationalization of compliance requirements. As programs come to fruition, many of these committees will likely transition to serve as points of escalation.

Technology-enabled compliance will likely be limited in nature with a range of tooling, from legacy tools to those procured from a wide array of third parties, in place to solve overlapping problems.


In the absence of cross-functional governance, boards of directors may find they are engaging directly in multidisciplinary governance for the first time.
An additional theme identified in organizations at the early stage of maturity was the absence of or lack of empowerment for a risk committee that coordinates enterprise risk management and board reporting on risk, digital governance or otherwise across the organization.
Board of directors
Audit committee
3RD LINE
Internal and/or external audit
While internal audits may be present in the third line, these functions will likely focus on financial controls rather than risk and control across a broad set of domains.
1ST/2ND LINE
Privacy committee
Cybersecurity committee
Technology committee
Legal committee
Data governance committee
Procurement committee
AI governance committee
Other domain leads
Privacy function
Security function
Technology
Legal
Data governance
Procurement
AI governance
Other domains
While these functions would traditionally sit solely within the second line, interviewees identified the absence of risk ownership and absence of subject matter expertise in the first line may mean the second line is expected to design and operationalize controls rather than advise, review and monitor them.
Business
Europe, Middle East and Africa
Asia-Pacific
Latin America
North America
EMEA legal and compliance
Asia-Pacific legal and compliance
LATAM legal and compliance
North America legal and compliance
A recurring theme among interviewees was the presence of committees with potentially overlapping remits and agendas and often inadequate diversity of disciplinary and expertise representation. Many committees were likely born out of status-reporting bodies set up as part of regulatory transformation programs and have continued in existence long after the completion of those programs.
In-scope domains will vary from organization to organization. Financial services organizations may have functions dedicated to preventing money laundering and fraud, while pharmaceuticals are more likely to have clinical trials teams. Each additional team may have a digital component that brings it under the digital governance umbrella.

Augmented governance

Enhanced governance enables better risk management.

An augmented model for an organization seeks to implement digital governance through various interdisciplinary processes and structures within a defined and structured approach to digital governance.

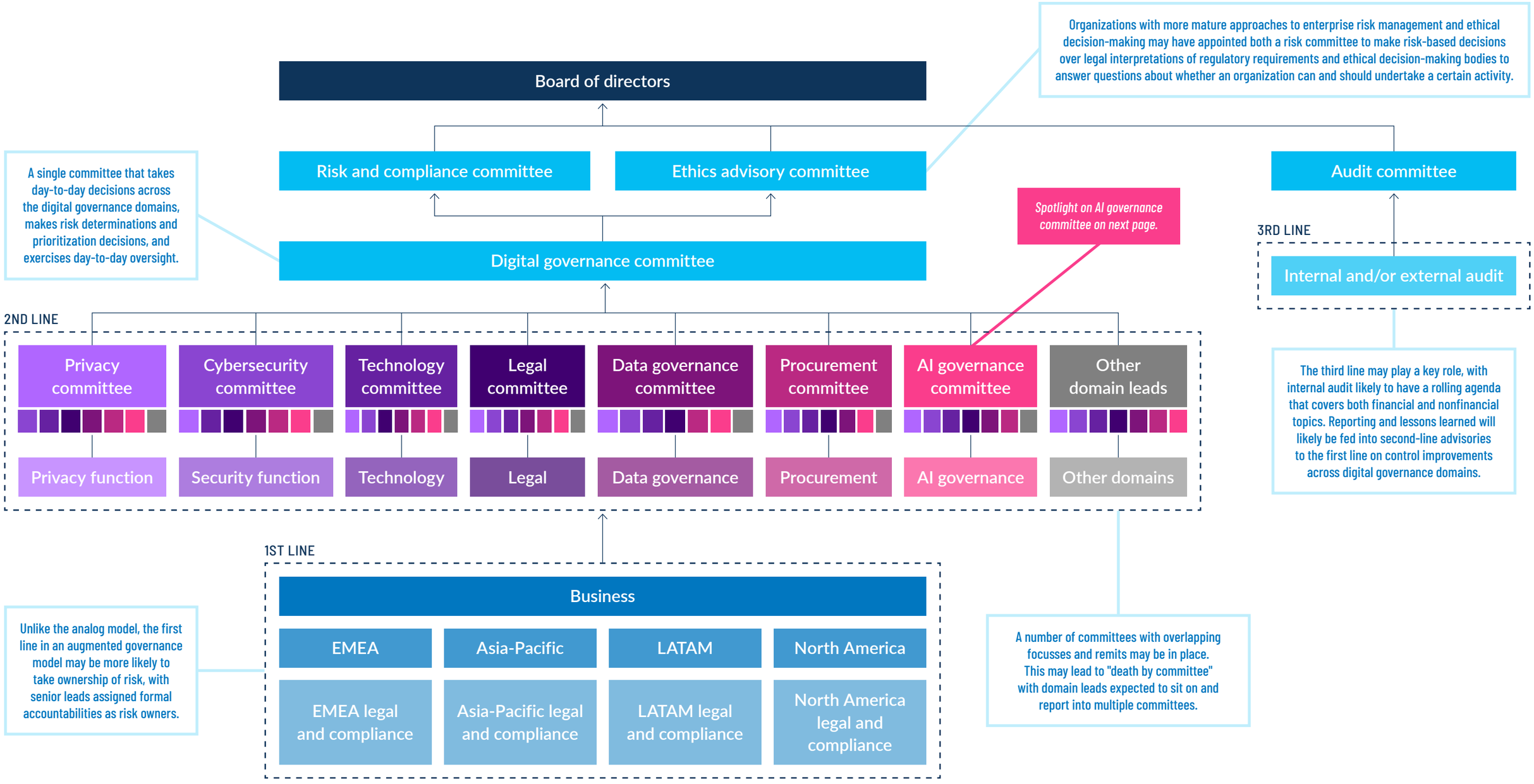
Senior leaders at organizations with more defined and/or mature approaches to digital governance identified a number of organizational structure characteristics and features that enable them to take a more coordinated approach to digital governance. These include:

→ Domain-specific committees chaired by domain leads, such as the CPO leading the privacy committee, with representation from additional domains as needed, such as attendance and reporting by the head of procurement into the privacy committee.

→ Emergence of AI governance giving prominence to the need for coordination between the commercial functions tasked with effective deployment of AI to meet business objectives and the compliance-driven functions grappling with the AI-governance requirements.

→ Greater awareness of risk and formalized responsibilities for risk decision-making within the first line, which enables the second line to take responsibility for monitoring and testing controls, rather than designing and operationalizing them.

→ Establishment of risk and data governance advisory committees. Risk committees may interpret law and policy requirements and approve risk-based decision-making, while data governance advisory committees support values-based decision-making to cover the "should we" and "could we" ethical decisions an organization may need to make.

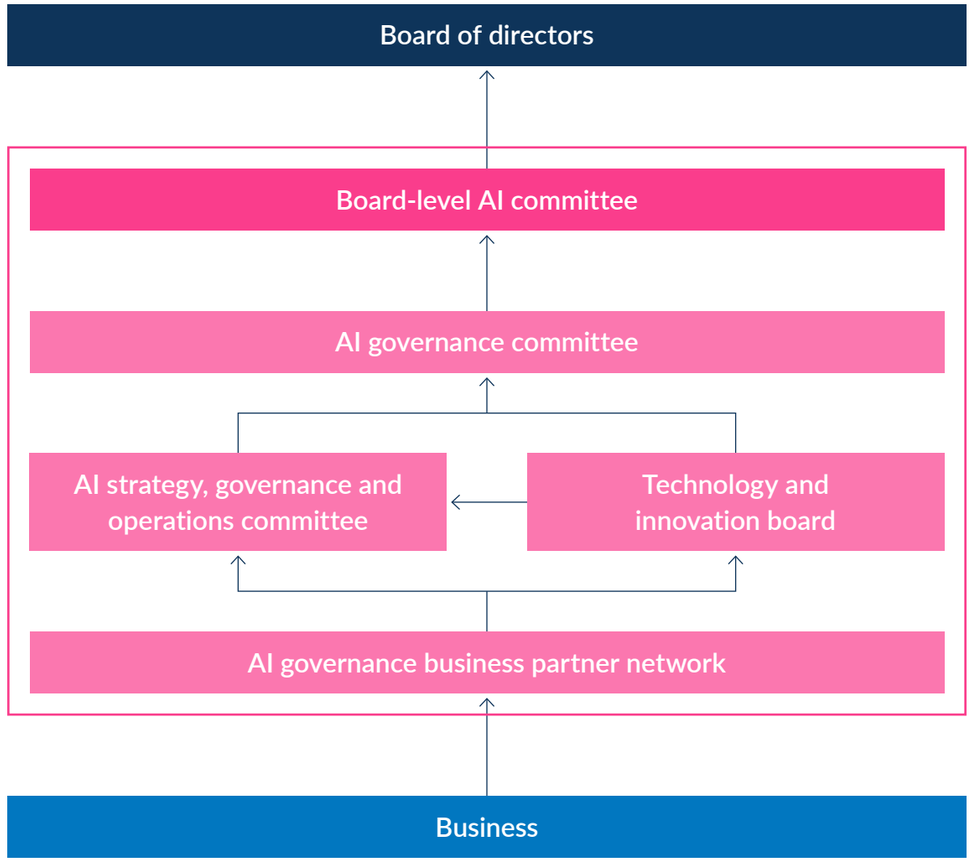

Organizations with more mature approaches to enterprise risk management and ethical decision-making may have appointed both a risk committee to make risk-based decisions over legal interpretations of regulatory requirements and ethical decision-making bodies to answer questions about whether an organization can and should undertake a certain activity.
Board of directors
Risk and compliance committee
Ethics advisory committee
Audit committee
A single committee that takes day-to-day decisions across the digital governance domains, makes risk determinations and prioritization decisions, and exercises day-to-day oversight.
Spotlight on AI governance committee on next page.
Digital governance committee
3RD LINE
Internal and/or external audit
2ND LINE
Privacy committee
Cybersecurity committee
Technology committee
Legal committee
Data governance committee
Procurement committee
AI governance committee
Other domain leads
The third line may play a key role, with internal audit likely to have a rolling agenda that covers both financial and nonfinancial topics. Reporting and lessons learned will likely be fed into second-line advisories to the first line on control improvements across digital governance domains.
Privacy function
Security function
Technology
Legal
Data governance
Procurement
AI governance
Other domains
1ST LINE
Business
EMEA
Asia-Pacific
LATAM
North America
EMEA legal and compliance
Asia-Pacific legal and compliance
LATAM legal and compliance
North America legal and compliance
Unlike the analog model, the first line in an augmented governance model may be more likely to take ownership of risk, with senior leads assigned formal accountabilities as risk owners.
A number of committees with overlapping focusses and remits may be in place. This may lead to "death by committee" with domain leads expected to sit on and report into multiple committees.

Spotlight on AI governance committees

As organizations grapple with rapid developments in AI, many organizations have made AI a strategic priority. In response, interviewees identified specific subgovernance structures have been set up to address AI strategy and AI governance, as the topic requires cross-functional expertise and collaboration. An example structure is included on the right.

A board-level AI committee has the ultimate accountability for decision-making and direction-setting regarding the organization's AI activities. The committee may be made up of senior leaders from across the organization who make day-to-day decisions, prioritizations and exercise oversight over AI use cases. Alongside this, an innovation board may conduct research and development activities for novel AI uses with the aim of keeping the organization's approach to AI ahead of its competition. An AI strategy, governance and operations committee may then address day-to-day decision-making on AI governance within the borders of the organization's broader AI strategy. These are both supported by an AI governance business partner network made up of individuals with AI governance expertise who may sit within the first line or between the first and second lines to support the design and operationalization of AI governance controls.

As AI governance programs mature, organizations may find they can transition these organizational structures to manage digital strategy and risk, with the aim of transitioning to a digital governance operating model.



Aligned governance

Coordination, coherence and consolidation across compliance domains may deliver better compliance outcomes.

An aligned model, representing a commonly aspired to future state for some organizations, seeks to streamline processes and structures into a more singularly defined and framed approach to digital governance.

As we look to the future, how might digital governance operating models mature? Automation, coordination, coherence among domains, centralization of subject matter expertise and decentralization of decision-making may play increasing roles. The following features may characterize an aligned digital governance operating model:

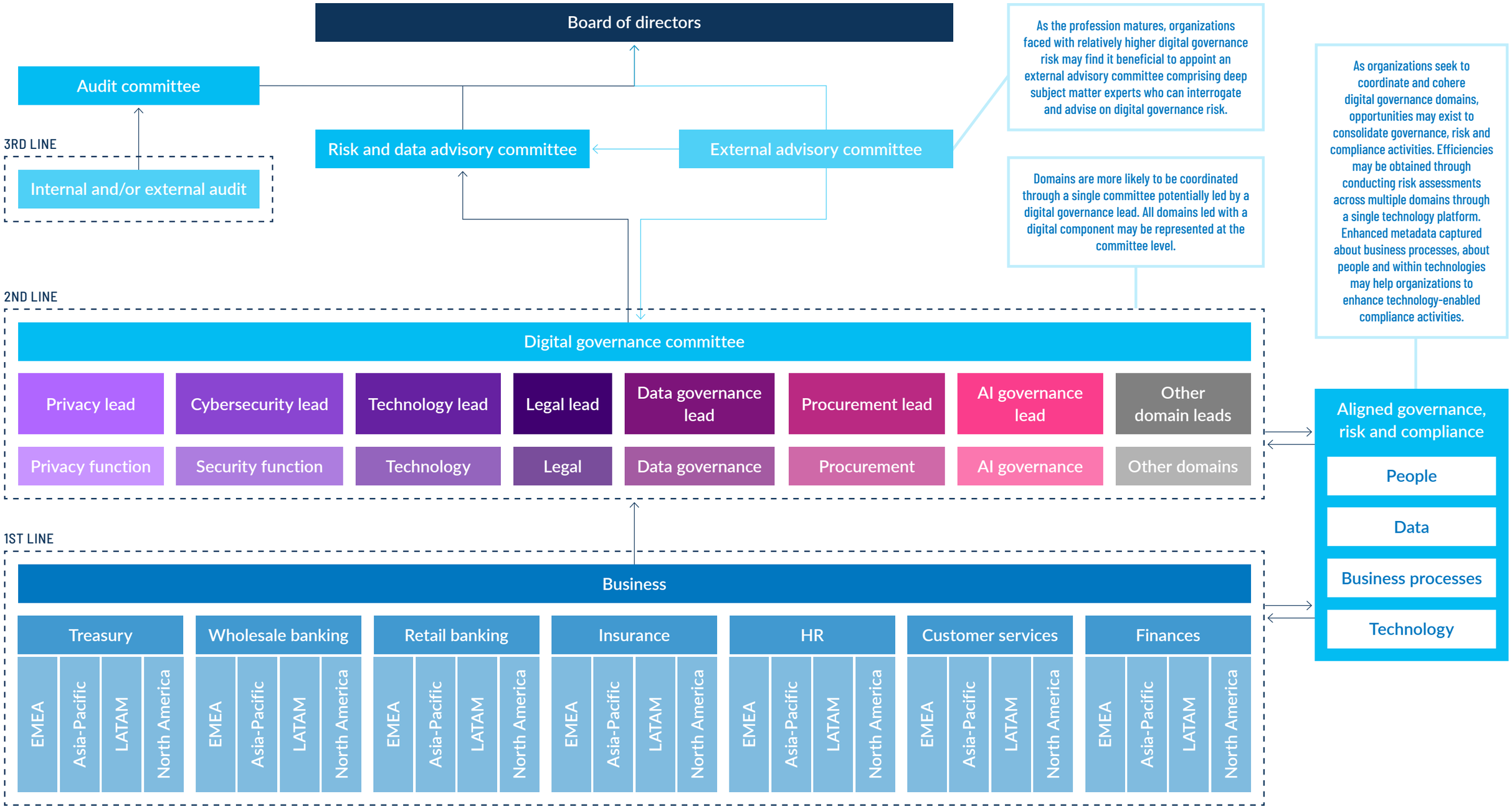
- → Increased automation in controls, coordination of governance activities and trust of various actors within the model.
- → Increased utilization of AI and business data to support enhanced reporting and decision-making.
- → Ability to use digital identities in a privacy-supporting manner to reduce friction in creating the transparency required for trust and verification.

- Multilateral and multimodal agreements in the supply chain, shifting away from bilateral analog contracts to smart contracts with enhanced and verifiable due diligence and algorithmic monitoring of contract performance post-contracting.

- Simplified policy frameworks within the organization that consolidate multiple data- and digital-related policies, underpinned by digital controls that combine multiple domain areas. Examples include a customer data retention control that considers privacy requirements alongside tax and financial reporting and an access control in the human resources department that considers the team alongside the purposes of processing to restrict access.

An aligned model seeks to streamline processes and structures into a more singularly defined and framed approach to digital governance.

While the specific digital governance model pursued by each organization will likely vary, the benefits of coordination, coherence and consolidation among compliance domains should be considered.


Board of directors
Audit committee
3RD LINE
Internal and/or external audit
Risk and data advisory committee
External advisory committee
As the profession matures, organizations faced with relatively higher digital governance risk may find it beneficial to appoint an external advisory committee comprising deep subject matter experts who can interrogate and advise on digital governance risk.
Domains are more likely to be coordinated through a single committee potentially led by a digital governance lead. All domains led with a digital component may be represented at the committee level.
As organizations seek to coordinate and cohere digital governance domains, opportunities may exist to consolidate governance, risk and compliance activities. Efficiencies may be obtained through conducting risk assessments across multiple domains through a single technology platform. Enhanced metadata captured about business processes, about people and within technologies may help organizations to enhance technology-enabled compliance activities.
2ND LINE
Digital governance committee
Privacy lead
Cybersecurity lead
Technology lead
Legal lead
Data governance lead
Procurement lead
AI governance lead
Other domain leads
Privacy function
Security function
Technology
Legal
Data governance
Procurement
AI governance
Other domains
Aligned governance, risk and compliance
People
Data
Business processes
Technology
1ST LINE
Business
Treasury
Wholesale banking
Retail banking
Insurance
HR
Customer services
Finances
EMEA
Asia-Pacific
LATAM
North America

Where to go and how to get there?

Organizations are carefully considering and curating approaches to bring order to digital entropy.

For many organizations, addressing the complex digital governance ecosystem is complicated, maybe even frustrated, by internal organizational structures and processes that are similarly complex to navigate and work through.

Senior leaders are thinking and working through issues from whether and how to define, design and implement improvements to how digital governance issues are managed by their organizations and how to bridge to the desired destination in ways that minimize disruption and do not expose the organization to new risks. Justifying changes to senior leadership and affected stakeholders is a core challenge and an enabler for the implementation of more effective digital governance.

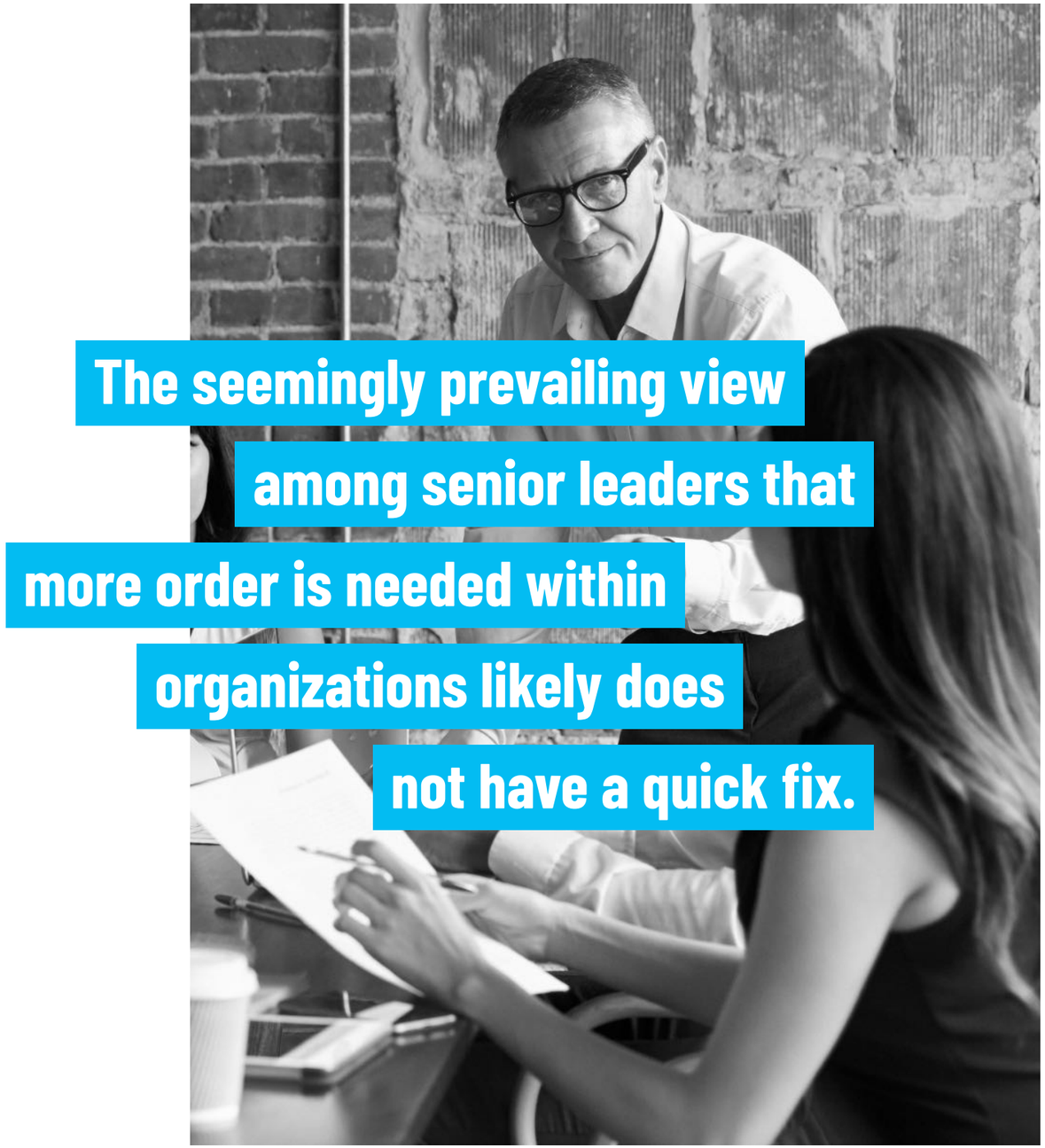
Cited benefits of establishing a more coherent digital governance model include:

→ **Improved clarity over digital strategy and compliance.** A coordinated and coherent digital governance model may enable senior leadership and committees to define roles, responsibilities, accountabilities and guidelines more clearly, including in ways that help translate the alphabet soup of digital governance regulation into practical implementation.

→ **Greater visibility and decision-making across the organization.** Clearer digital governance structures may provide senior leadership with lines of sight into increasingly important digital risks and critical compliance requirements. In turn, that may empower more timely and better informed decision-making and risk-management processes. Establishing a digital governance model with underlying policies, procedures and technologies can enable specification and identification of the information required by the board and its committees, as well as from whom, how often and under what circumstances they receive that information.

→ **Improved coordination across digital governance subdomains.** The complexity inherent within and between digital governance subdomains may be compounded by challenges faced in coordinating across distant or disparate parts of the organization. Cohabiting the strategic decisions, compliance responses and values-based decision-making in a more aligned model may mitigate these challenges and avoid both unaddressed risks and inefficient duplication of efforts.

Justifying changes to senior leadership and affected stakeholders is a core challenge and an enabler for the implementation of more effective digital governance.



The seemingly prevailing view among senior leaders that more order is needed within organizations likely does not have a quick fix. This is especially true if it is to endure the continuously changing digital governance ecosystem. Some of the key challenges discussed include:

→ **Resource constraints.** Improving organizational capacity and capability can require significant effort and expertise, which not all companies have. Finding time to add more work streams to already burdened functions and finding, attracting, training and retaining the very small number of experts were common specific challenges cited by senior leaders. This will likely be a particularly acute challenge for micro-, small- and medium-sized organizations.

→ **Challenges in getting buy-in across functions.** Working with, across and through different subject matters and disciplines is challenging. Many organizational functions have entrenched ways of working. Changing the status quo, promoting a shared lingua franca and breaking down silos are all likely to unsettle functions.

→ **Lack of benchmarking.** In the near to medium term, it is unlikely one-sized approaches within industries or use cases will proliferate. This makes it hard for organizations to benchmark to and learn from their industry peers and competitors. Organizations, with their own distinct cultures, structures, footprints and strategic priorities, will each seek their own way forward. That said, over time, organizations will seek to benchmark certain practices to their industry peers and to regulatory expectations, as is the case today with enterprise risk management.

- **Greater reliance on digital technologies.** As organizations become more digital, more reliance will be placed on existing processes and technologies. That might make it harder to justify and effect departures from the organizational governance status quo. Organizations may therefore need to take steps to establish resilience in their digital architectures and supply chains.

- **Velocity and vibrancy of change.** The accelerating, dynamic and often uncertain development of digital technologies and their applications will likely result in an underestimation of the complexity and potential impacts of the corresponding governance approaches required. The ability of approaches to adapt, potentially often and to significant degrees, may prove challenging to the ongoing efficacy of an organization's digital governance efforts.

Many organizations are at the beginning of a likely long journey to recast their approaches to governing the application of digital technologies. That long journey will likely take place over a relatively short period, repeating and iterating over time. As many senior leaders remarked, this is the future of our profession.

Contacts

Connect with the team

Saz Kanthasamy
Principal Researcher, Privacy Management, IAPP
skanthasamy@iapp.org

Joe Jones
Director of Research and Insights, IAPP
jjones@iapp.org

Lynsey Burke
Research and Insights Project Specialist, IAPP
lburke@iapp.org

Follow the IAPP on social media

Published September 2024.