Organizational Digital Governance Report 2025

Table of contents

What's inside?

Foreword ii

Introduction 1

Part I. Navigate digital risk index 2

Part II. Mapping digital governance domains 19

Part III. Maturing digital governance functions 25

Part IV. Regulatory risk or reward? 35

Part V. Governance driving innovation 42

Looking ahead 53

Our research approach 54

Contacts 55

Foreword

Deciphering digital governance

A Rosetta Stone for digital governance

Discovered in rubble over 200 years ago, the Rosetta Stone is one of the most important, visited and mysteriously enticing artifacts related to ancient Egypt. Its epigraphical significance in deciphering Egyptian hieroglyphs alongside Demotic script and Ancient Greek text unlocked history and knowledge from the ancient world.

But the Rosetta Stone is more than a tool in the science of history. It is also more than an idiomatic expression for the notion of a keystone to encoded, hidden or lost knowledge.

There is something for the ages about this seemingly primitive, dark, roughly cut and fractured slab of stone with its scratched inscriptions that speaks to the human and societal condition. It speaks to our yearning and conditioned instinct to search for greater actionable understanding of a larger whole as we journey into the future, a theme captured in H.G. Wells' 1933 dystopic science fiction novel "The Shape of Things to Come."

As organizations journey into a future of digital entropy — a state of disorder by dint of the complexities associated with the intersecting, overlapping and even conflicting domains and disciplines for the governance of digital technologies — they too are searching for ways to decode, translate and build more navigable and holistic responses. Organizations aim to find ways to bring order to the entropic — through structure, a shared frame of reference and through professionalism.

Making sense of this multi-domain, multi-disciplinary and increasingly multi-polar world of digital governance is not just an exercise in translation and resolving complexity. The saved costs and reduction in risks that come with deciphering the Rosetta Stone for digital governance show up on just one, albeit one important, side of the ledger for organizations. The other side of the ledger — increasingly in focus for business leaders, politicians and more broadly our societies and economies — is how to increase growth and innovation and how to sustain success in a competitive digital ecosystem.

One of the beauties of the Rosetta Stone is in how it provides a path to bridge — not displace — the immensely deep, storied and diverse histories and traditions of the Egyptians and Greeks. In the areas of privacy, artificial intelligence governance, cybersecurity and online safety, for example, there is, and will remain, the need for specialists but, crucially, not siloed expertise and functions; and there will continue to be dedicated research on the governance of specific domains and disciplines.

This year's Organizational Digital Governance Report documents the extent to which organizations are deciphering their own Rosetta Stones in bringing together previously disparate or disconnected functions, governance programs and domains. Organizations are constructing something more whole than its constituent parts. They are leveraging approaches that enable better risk management, risk-taking, and opportunity seizing. They are prioritizing efforts to give language and meaning, as well as order, to the professional practice of organizational digital governance.



Joe Jones
Director of Research and Insights, IAPP



Introduction

Since 2015, the IAPP has surveyed the growing global community of professionals to determine the state of privacy governance within organizations. The unrelenting and dynamic growth of digital technology has brought with it a developing, broadening and consequential aperture through which digital technologies are to be governed.

It is no longer sufficient to view digital organizational governance within the siloed context of privacy. AI governance, online safety and cybersecurity — just to name a few domains — are also crucial. The interplays and intersections between these domains from a regulatory, societal, technological and market perspective drive how organizations approach digital governance.

Recognizing this, the IAPP published a report in 2024 focused on organizational digital governance and coined the term "digital entropy." We sought to determine the extent to which organizations were feeling the effects of an increasingly entropic digital governance environment and how they were responding. The 2024 report documents how organizations leveraged and evolved already-established governance structures and were beginning to integrate several different digital domains in response.

The 2025 governance survey sought responses from the IAPP's global membership base to a 74-question survey over the course of eight weeks from April to June 2025. Questions sought to elicit information on the extent to which organizations are defining, designing and deploying digital governance programs and, in practical terms, how they are doing so. More than 600 individuals from 45 countries and territories responded.

The IAPP will be publishing additional content specific to the governance structure of individual domains, such as privacy governance, that will more closely examine topics such as team size, budget, recruiting and use of technology.

Part I. Navigate digital risk index

Classifying the organizational digital risk environment

Whereas threats to commerce, governance and daily life used to be local and proximate to the source of danger — think being at the foot of Mount Vesuvius in 79 AD or Pudding Lane in London in September 1666 — today's digitally-driven world is hyperconnected and smaller with the risks having further-reaching consequences. The risk environment for digital technologies remains inherently complex, ever changing and, in the absence of proactive risk management, difficult to navigate.

In January 2025, the IAPP surveyed its members alongside select high-level global digital policy leaders attending the 2025 Navigate Digital Policy Leadership Retreat the IAPP co-hosted with the Berkman Klein Center at Harvard University. We invited their assessment of the top risks driving and shaping the design, deployment and governance of digital technologies now and in the near-term. Given the volume and variety of risks to choose from, respondents selected the most important risks in four different, albeit related, categories: geopolitical, organizational, technological, and societal and environmental.

The risk environment for digital technologies remains inherently complex, ever changing and, in the absence of proactive risk management, difficult to navigate.

Top 10 digital risks across categories, overall

Digital risk	Percentage indicated	Category
Risk to privacy and data protection	58%	Societal and environmental
AI technologies as accelerating or compounding the risk of adverse outcomes	54%	Societal and environmental
Dependency on and risks associated with third-party vendors	51%	Technological
Lack of sufficient budget and resources to invest in governance professionals, practices and tooling	48%	Organizational
Nation state or sponsored cyberattacks, espionage and warfare	42%	Geopolitical
Legacy infrastructure and tooling unfit for purpose	41%	Technological
Political and policy focus on deprioritizing governance and compliance	39%	Geopolitical
Unclear or lack of awareness of data and systems mapping	39%	Technological
Identifying and managing misinformation and disinformation online	37%	Social and environmental
Business deprioritization of governance and compliance, e.g., towards innovation, monetization and competitiveness	36%	Organizational

Note: Overall percentages in this section are representative of the more than 600 global digital responsibility leaders polled for the Navigate Digital Risk Index. Additional insight is provided — in the form of demographic analysis — with data from the subset of respondents who participated in the 2025 governance survey and provided such information.

Identified risks span categories, demonstrating how varied and broad the risk landscape is. Many risks resonate across different organizational demographics, such as cybersecurity-related risks, which topped the list across many demographics. Combined with the fact that 62% of respondents reported experiencing a security incident and/or data breach over the past year, it is easy to see how and why cybersecurity risks outrank many others.

For example, 76% of respondents in the government sector identified being concerned about privacy and data protection risks — far more than the overall average —whereas only 47% of those in the technology and telecommunications sector indicated this as a risk. On the other hand, the government sector was significantly less likely to indicate misinformation/disinformation as a risk at 21%, whereas the technology and telecommunications sector aligned more with the overall averages at 33%.

Differing risk assessments are also present by continent. Respondents from Asia were significantly less likely than average to identify data awareness and systems mapping as a risk, but more likely than average to identify budgetary issues as risks — at 18% and 64%, respectively.

These demographic differences suggest that while there may be overall agreement of the top digital risks organizations are facing, risk perception may be heightened or lowered by key factors related to that organization's setting and industry.

In addition to demographic differences, it's important to frame and reframe the concept and assessment of risk through the eye of the beholder. Different roles within organizations will view digital risk management and risk-taking differently.

Business leaders, not surprisingly, tend to see risk through a strategic and tactically comparative, if not competitive, lens, with a strong eye on growth and innovation. For them, digital risks are often tied to long-term outcomes: regulatory readiness, reputational integrity and resilience in the face of changing expectations. Operational teams, by contrast, may focus more on the immediacy of implementation challenges. Compliance professionals may view risk as derivative from law and policy.

The multidimensional, multi-layered and multi-domain shape to digital risk makes building and implementing coherent organizational governance an imperative for many.



Exploring risks by category

Each risk category contains ten separate risks, for a total of forty risks that frame the Navigate Digital Risk Index. Each risk category is explored below.

Geopolitical
Nation state or sponsored cyberattacks, espionage and warfare
Political and policy focus on deprioritizing governance and compliance — e.g., towards innovation, monetization and competitiveness
Economic competition and confrontation, including through political directives that protect or prefer certain providers of digital technologies over others
Risks to human rights and/or civic freedoms associated with political, policy and regulatory interventions on digital governance
Increasingly multipolar, siloed or fragmented governance norms and rules
Disruption to cross-border data flows
National security interests, concerns and risks impacting digital governance — e.g., the design of digital technologies and access to data
Increasingly multipolar or fragmented approaches to regulatory enforcement
Concentration of, dependency on, or unequal access to foreign technology, services and resources
Heightened consumer reaction and activism directed at individual organizations and nations

Organizational
Lack of sufficient budget and resources to invest in governance professionals, practices and tooling
Business deprioritization of governance and compliance — e.g., towards innovation, monetization and competitiveness
Lack of or unclear accountability and ownership of risk management and risk-taking
Lack of access to or availability of skilled governance talent — e.g., legal, compliance, management and technical
Legacy or insufficient data governance management architecture and processes
Siloed governance structures and functions, especially along domain lines — e.g., privacy, AI governance and cybersecurity as siloed functions
Difficulty navigating and reconciling the volume, variety and complexity of legal obligations
Lack of awareness, literacy and empowerment on effecting organizational policy and requirements
Challenges designing, building and implementing scalable governance solutions across different markets
Distance from and lack of empowerment by senior leadership

Societal and environmental
Risk to privacy and data protection
AI technologies as accelerating or compounding the risk of adverse outcomes
Identifying and managing misinformation and disinformation online
Challenges in defining and measuring potentially harmful impacts of technology
Risk of discrimination, bias and unfairness
Decline of societal stability, increase in fragmentation and polarization
Risk of outsized harmful impacts on children, the vulnerable, and marginalized people and communities
Concentration of, or unequal access to, technology and information across society, along demographical lines
Lack of empowerment to effect rights and access effective remedies
Declining access to sufficient energy or the impact on energy consumption

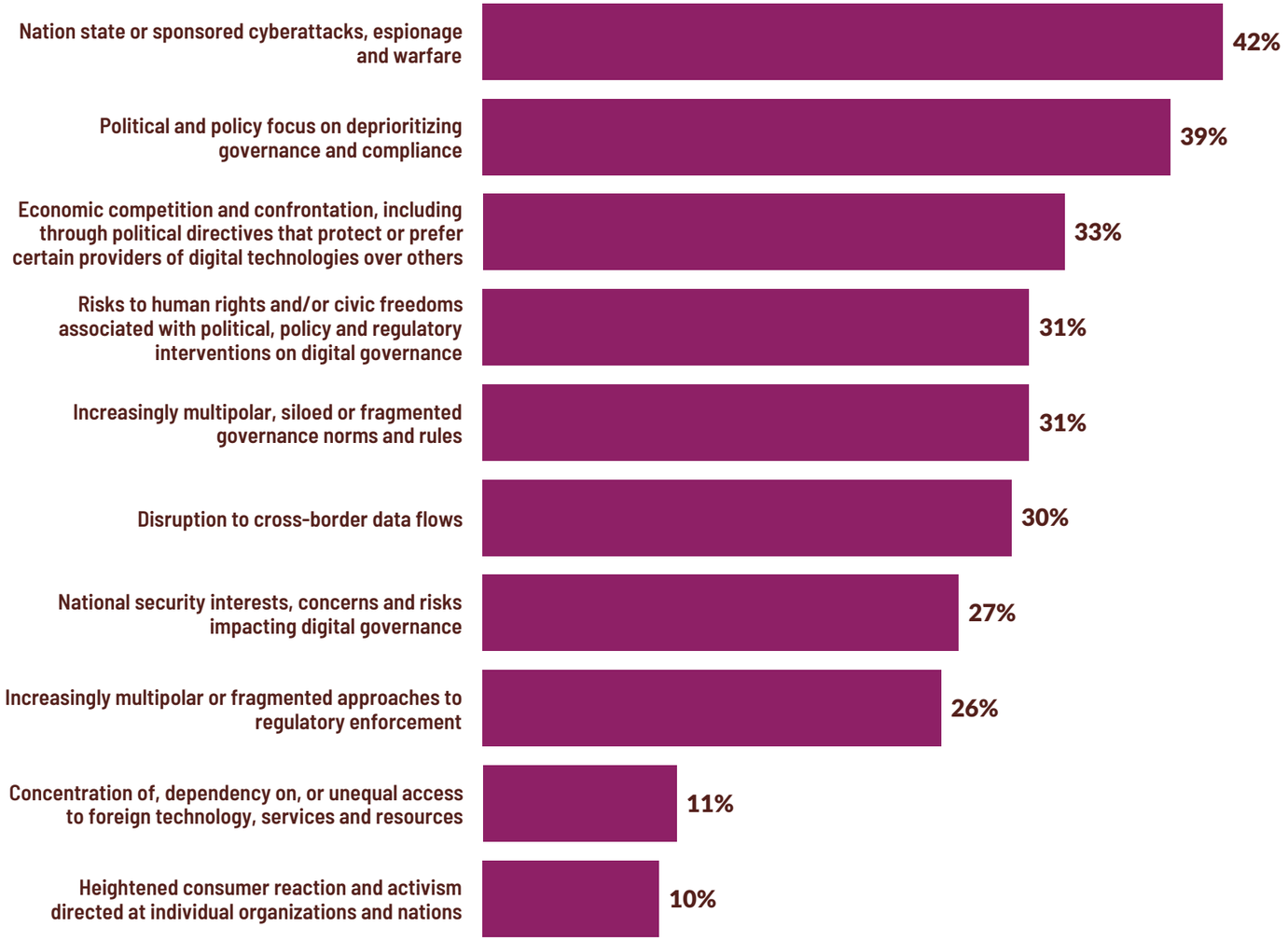
Technological
Dependency on and risks associated with third-party vendors — e.g., supply chain vulnerabilities
Legacy infrastructure and tooling unfit for purpose
Unclear or lack of awareness of data and systems mapping
Ensuring physical and cybersecurity and resilience
Pace of innovation and technological change causing technological obsolescence
Engineering governance into design or by default
Challenges aligning technology with organizational and business goals
Decreased safety and reliability given changing technological state of the art
Selection, integration and management of compliance-tech and governance-tech vendor solutions
Engineering governance into post-design and deployment

Geopolitical

Geopolitical digital risks refer to those emanating from international political forces, global power dynamics and the interplay between different national policies. They can originate from political decisions, cross-border tensions and international regulations that affect how digital technologies are developed, deployed or governed. Digital policy matters have increasingly been at the front line of global geopolitical developments, from international trade to national security, and are regular matters which political leaders contend with.

When coupled with other factors, a respondent's top geopolitical risk varied, in some cases quite significantly, especially by jurisdiction of the headquarters of the organization. Organizations headquartered in South America, for instance, are significantly more concerned compared to other jurisdictions about increasingly fragmented approaches to regulatory enforcement, whereas organizations headquartered in Africa are more concerned, on average, with cross-border data flow issues.

Top geopolitical digital risks, overall



Top geopolitical digital risks, by headquarter location

Risk	Overall	North America	Europe	Asia	South America	Africa	Oceania
Nation state or sponsored cyberattacks, espionage and warfare	42%	44%	49%	32%	29%	17%	47%
Political and policy focus on deprioritizing governance and compliance	39%	43%	39%	45%	43%	17%	47%
Economic competition and confrontation, including through political directives that protect or prefer certain providers of digital technologies over others	33%	33%	37%	27%	43%	33%	20%
Risks to human rights and/or civic freedoms associated with political, policy and regulatory interventions in digital governance	31%	33%	32%	45%	43%	33%	33%
Increasingly multipolar, siloed or fragmented governance norms and rules	31%	34%	21%	23%	0%	17%	27%
Disruption to cross-border data flows	30%	25%	33%	36%	29%	50%	20%
National security interests, concerns and risks impacting digital governance	27%	27%	20%	32%	29%	17%	40%
Increasingly multipolar or fragmented approaches to regulatory enforcement	26%	28%	22%	9%	71%	33%	13%
Concentration of,dependency on, or unequal access to foreign technology, services and resources	11%	6%	20%	14%	14%	50%	7%
Heightened consumer reaction and activism directed at individual organizations and nations	10%	13%	6%	14%	0%	0%	20%

> **In Argentina, we're seeing increased regulatory attention on AI and automated decision-making, pushing organizations to rethink how governance intersects with fairness, transparency and explainability. Across Latin America, different legal frameworks have made interoperability and accountability key challenges — particularly for companies operating regionally or expanding globally.**
>
> Diego Fernández
> Partner, Marval O´Farrell & Mairal

While geopolitical risks can threaten to destabilize operations and cause compliance burdens, geopolitics can also present strategic opportunities for organizations in the form of mergers and expanding into different markets. This is especially true in cases where organizations can leverage comparative operational and innovative global differences and even volatility in their favor.

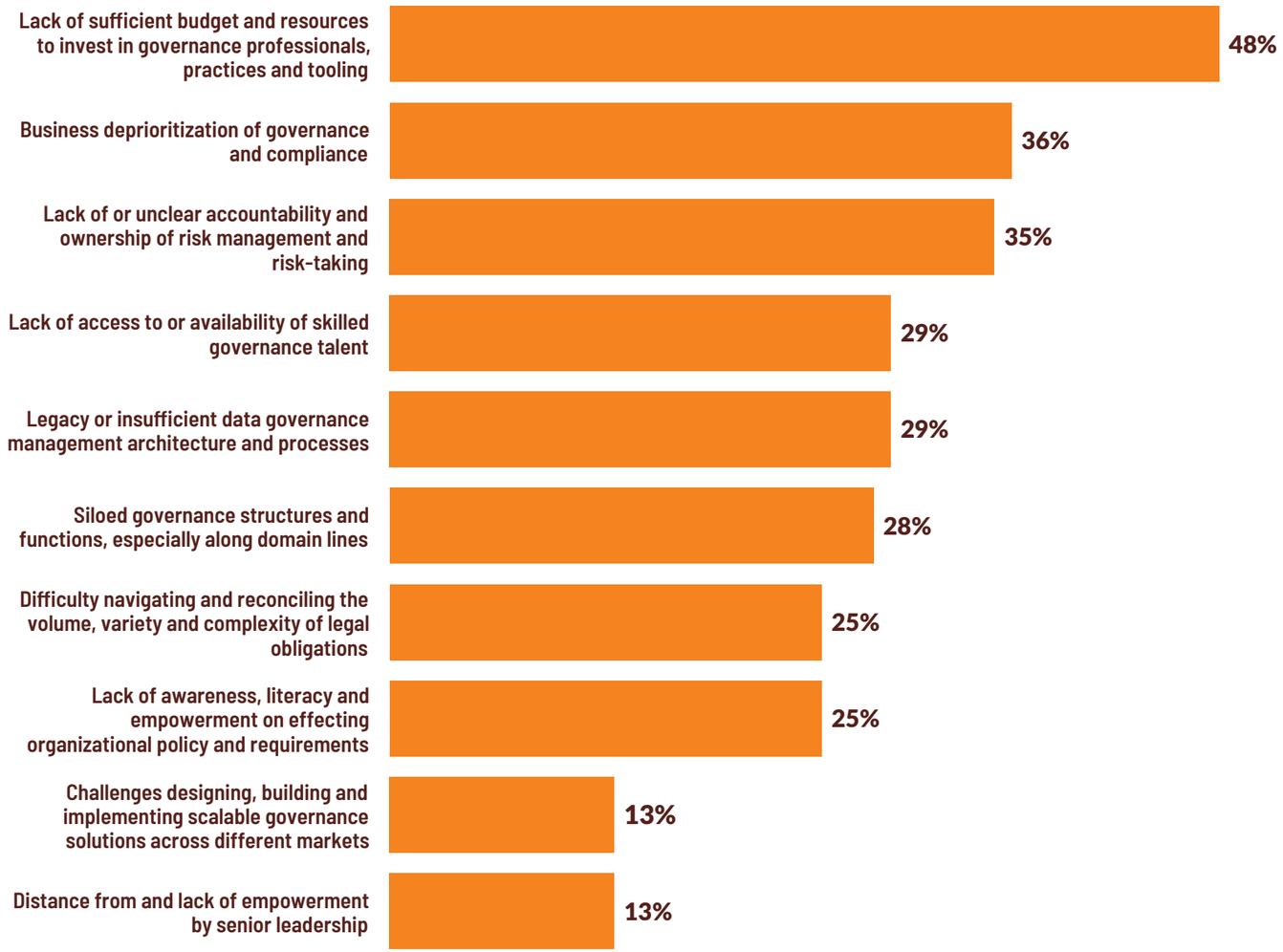


Organizational

Organizational digital risks arise from internal structures, processes, culture and resource decisions that affect how well a company manages its digital operations, data and technologies. They are typically driven by people, policy or process.



Top organizational digital risks, overall



Top organizational digital risks, by headquarter location

Risk	Overall	North America	Europe	Asia	South America	Africa	Oceania
Lack of sufficient budget and resources to invest in governance professionals, practices and tooling	48%	54%	45%	64%	57%	33%	73%
Business deprioritization of governance and compliance	36%	38%	40%	27%	43%	0%	40%
Lack of or unclear accountability and ownership of risk management and risk-taking	35%	33%	36%	27%	43%	17%	20%
Lack of access to or availability of skilled governance talent	29%	24%	29%	41%	71%	50%	33%
Legacy or insufficient data governance management architecture and processes	29%	32%	31%	32%	0%	50%	20%
Siloed governance structures and functions, especially along domain lines	28%	29%	29%	14%	29%	33%	40%
Difficulty navigating and reconciling the volume, variety and complexity of legal obligations	25%	25%	31%	27%	0%	17%	13%
Lack of awareness, literacy and empowerment on effecting organizational policy and requirements	25%	27%	22%	18%	43%	50%	13%
Challenges designing, building and implementing scalable governance solutions across different markets	13%	13%	8%	9%	14%	17%	27%
Distance from and lack of empowerment by senior leadership	13%	12%	15%	9%	0%	0%	7%

Even within industry, the type of business the organization engages in informs digital risk perception. For example, only 29% of those in the business-to-business sector, compared to the overall average of 37%, identified a lack of or unclear accountability and ownership of risk management and risk-taking.

Interestingly, 78% of the respondents who confirmed that in a scenario where digital governance is deregulated, their organization would continue to invest in and deliver on governance activities also identified siloed governance structures and functions as a top digital risk. This further reinforces that organizations recognize the benefit of governance frameworks beyond regulatory compliance.

Only 29% of those in the business-to-business sector, compared to the overall average of 37%, identified a lack of or unclear accountability and ownership of risk management and risk-taking.



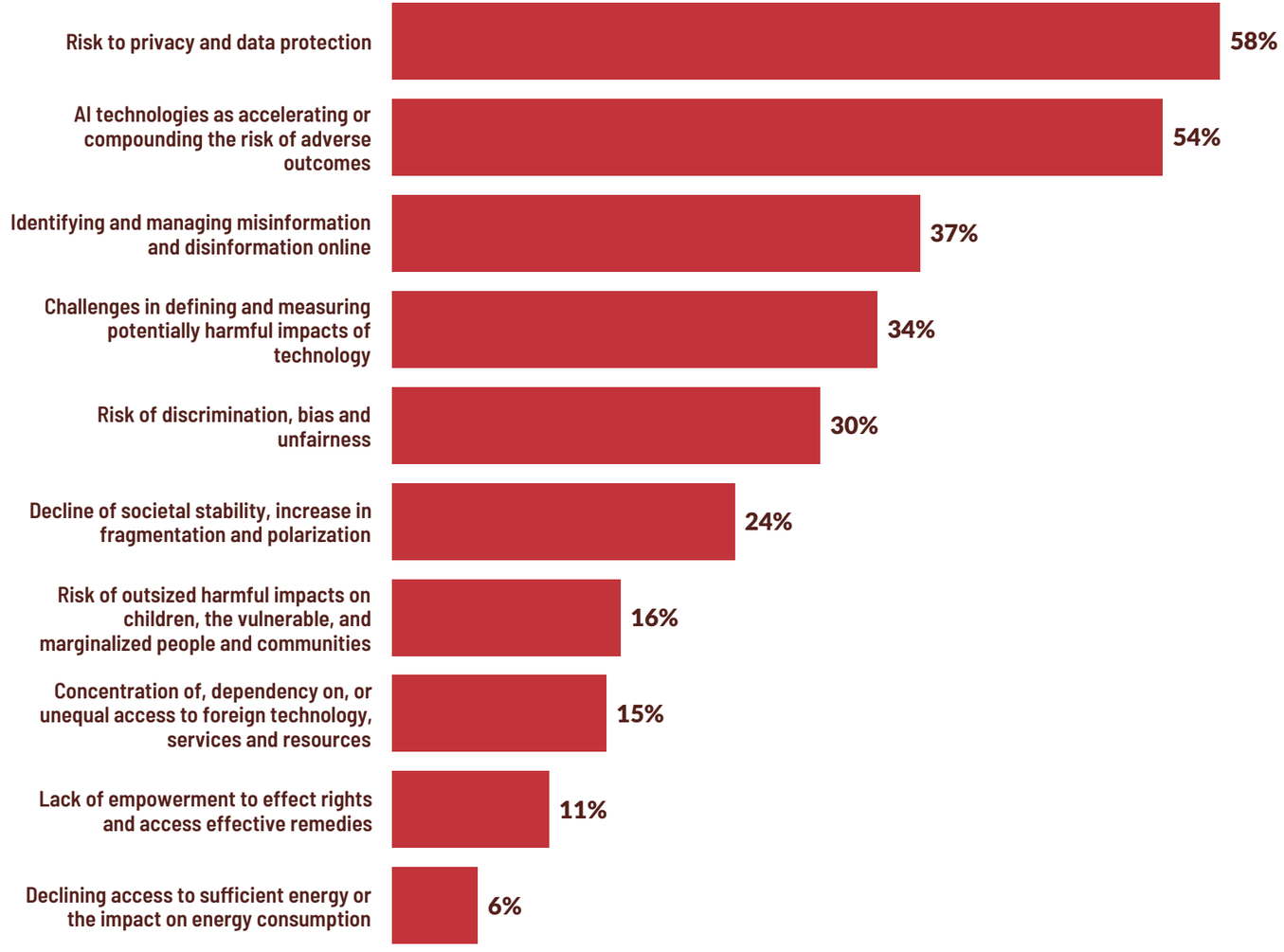
Societal and environmental

Societal and environmental digital risks arise from the broader impact of digital technologies on society, culture and the environment and, in turn, how that impact informs the risks associated with the design and deployment of digital technologies. This category of risks includes how public perception, ethical concerns and embedded social dynamics can affect an organization's ability to operate. It also reflects the perceived sense of trust society and customers place in the organization as well as its long-term viability and sustainability in leveraging digital technologies.

Often, these risks illustrate how the use or misuse of digital systems could influence communities, people and the planet.

The societal and environmental digital risk category contained the top two overall digital risk responses among our survey respondents: 58% noted a risk to privacy and data protection and 54% reported the risk of AI technologies as accelerating or compounding potential adverse outcomes. These selections were also not mutually exclusive; 57% of respondents who identified risk of AI technologies also selected risk to privacy and data protection and 50% of those who selected risk to privacy and data protection also selected risk of AI technologies.

Top societal and environmental digital risks, overall



Top societal and environmental digital risks, by headquarter location

Risk	Overall	North America	Europe	Asia	South America	Africa	Oceania
Risk to privacy and data protection	58%	64%	57%	45%	57%	67%	60%
AI technologies as accelerating or compounding the risk of adverse outcomes	54%	56%	48%	50%	43%	50%	53%
Identifying and managing misinformation and disinformation online	37%	39%	38%	36%	43%	33%	27%
Challenges in defining and measuring potentially harmful impacts of technology	34%	31%	37%	59%	43%	33%	40%
Risk of discrimination, bias and unfairness	30%	29%	31%	27%	43%	17%	27%
Decline of societal stability, increase in fragmentation and polarization	24%	25%	30%	9%	0%	33%	0%
Risk of outsized harmful impacts on children, the vulnerable, and marginalized people and communities	16%	14%	20%	14%	14%	0%	13%
Concentration of, or unequal access to, technology and information across society, along demographic lines	15%	12%	13%	27%	29%	50%	40%
Lack of empowerment to effect rights and access effective remedies	11%	9%	11%	23%	0%	0%	13%
Declining access to sufficient energy or the impact on energy consumption	6%	7%	6%	0%	29%	0%	7%

> **In an increasingly fragmented, and ever-changing, digital regulatory landscape, the real competitive edge for organizations lies in finding common ground. While a true one-size-fits-all, jurisdiction agnostic, model for digital governance may remain aspirational, multinational companies can — and must — strive for a harmonized core framework that respects and even leverages local nuance and risk, without sacrificing global coherence. This will promote both good compliance levels without sacrificing efficient adoption of new technology across a business. The future belongs to those who can operationalize trust, transparency and accountability across borders, not just within them.**
>
> Alexander Milner-Smith
> CIPP/E, partner, Lewis Silkin LLP

By region, respondents from Asia, South America and Oceania are much less likely to indicate a decline in social stability/increase in polarization as a top digital risk compared to other regions. Additionally, respondents from Africa are also less likely to indicate a risk of discrimination, bias or unfairness.

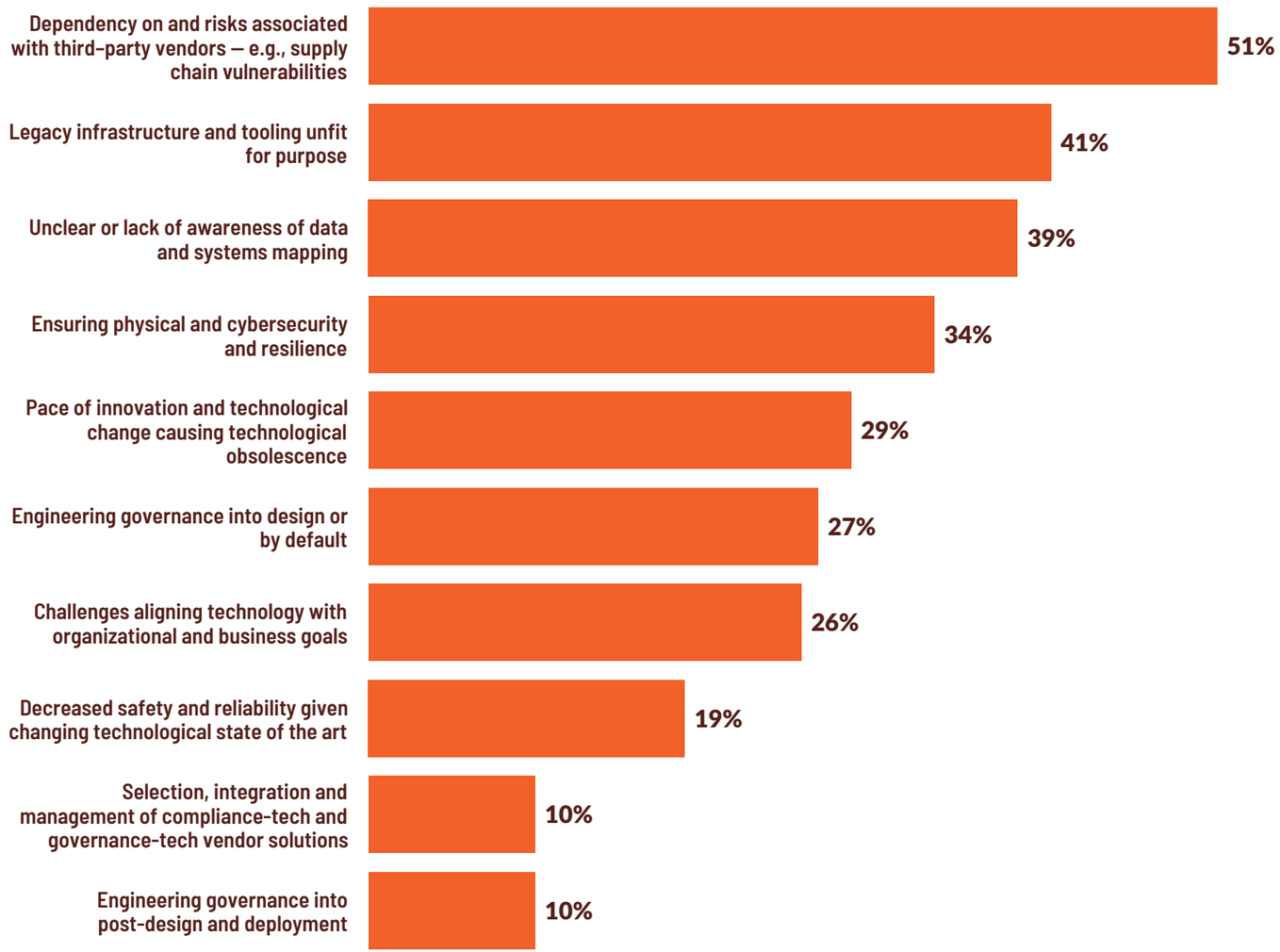
On the other hand, over half of respondents from Asia identified the risk of defining and measuring harmful impacts of technology as significantly higher than the average of 34%. It is unsurprising that societal and environmental risks are perceived differently across geographies of the world, demonstrating the risk associated with diverging approaches shaped by diverse contexts and cultures that inform a digital governance approach.

Technological

Technological digital risks refer to those stemming from digital systems, infrastructure, tools or technical architecture. Often, these risks concern the security, predictability or efficacy of the tools and systems offered or used to empower the digital aspects of an organization's operational delivery.

Risks evolve as technology and systems assume new roles and importance within organizations. The need for employees who understand and are experts in specific technologies typically grows as the technology becomes more complex, integrated and consequential to success or failure.

Top technological digital risks, overall



However, true understanding can be hard in the face of complexity. For example, over half of respondents who identified unclear or lacking awareness of data and systems mapping as a top technological risk also reported they are not confident senior leaders in their organization understand and/or appreciate how their role can be enabled for innovation and growth.

Of respondents who reported challenges aligning technology with organizational and business goals as a top digital risk, 83% believe regulation is helpful to the mission of using data and digital technology for innovation and achieving business outcomes. This correlation could mean that organizations use the guardrails of regulation to help prioritize and gain leadership attention, leveraging investment in compliance to better align technology to their organization's goals.

Given the ever-growing role of technology within cyber and national security, overlapping considerations between technological and geopolitical risks occurred for many respondents.

Comparison of technological risks to select geopolitical risks

Technological risk	Overall	% of these respondents that chose selected geopolitical risk
Legacy infrastructure and tooling unfit for purpose	41%	45% / 43%
Decreased safety and reliability given changing technological state of the art	19%	50% / 41%
Challenges aligning technology with organizational and business goals	26%	38% / 41%
Ensuring physical and cybersecurity and resilience	34%	61% / 37%
Pace of innovation and technological change causing technological obsolescence	29%	37% / 40%
Engineering governance into design or by default	27%	45% / 47%
Engineering governance into post-design and deployment	10%	36% / 53%

% of respondents who also chose "Nation state or sponsored cyber-attacks, espionage and warfare"

% of respondents who also chose "Political and policy focus on deprioritizing governance and compliance"

Case Study - Nubank - Appointing an AI governance working group

As a digital financial technology company, Nubank places AI at the core of its mission: to fight complexity and empower people. The company leverages AI to support its customers' complete financial journey, promote financial inclusion, and advance responsible and transparent lending. Operating in a heavily regulated market, Nubank balances its commitment to AI-driven innovation with regulatory compliance and a proactive approach to mitigating potential risks for individuals.

Nubank's journey in managing AI risks began even before a formalized AI governance framework was established. The company has long had dedicated defense teams that managed risks related to models, data privacy and information security. This structure stems from financial market best practices, data protection laws, and Brazilian Central Bank requirements on risk management — including model risk management — and information security.

Although existing risk management and governance processes were primarily designed for traditional AI, such as regression and tree-based models, they provided the foundational guardrails for "emerging AI" like generative AI and large language models.

To address the escalating complexities of emerging AI and the need for centralized oversight, Nubank formed the AI Governance Working Group to unify its existing risk management processes. Serving as Nubank's official AI Risk Steward, this global, multi-disciplinary team brings together senior members from data protection, legal, IT risk, information security and model risk, as well as partners from procurement and business/platform teams. Its core role is to closely monitor internal AI use, track external trends and ensure robust risk management.

The AIGWG leverages existing risk management frameworks rather than creating new ones. This philosophy led to the formal establishment of the AI Risk Management Guidelines in 2024, which streamline risk assessment across the AI life cycle, from testing and development to procurement and usage. By stitching together core defense functions, this integrated approach simplifies risk management and enhances team collaboration while minimizing bureaucracy to AI users and developers, directly fostering an environment of innovation.

The AIGWG and its approach have continuously evolved as new risks arise from the increasing adoption of emerging AI. For instance, as the number of requests for proof of concepts with AI vendors grew, the AIGWG collaborated with the procurement department to embed its defense risk assessment flows directly into the PoC request process. This integration means business teams no longer need to open separate requests for AI risk assessments and legal agreements for PoCs.

Lastly, reflecting its heavily regulated environment and three-lines-of-defense risk model, Nubank's AI governance is deeply embedded within existing operational procedures. For example, when integrating an AI system into a product, personnel follow the standard new products and features process, which automatically triggers assessments by relevant defense teams. Additionally, developing an AI model necessitates adherence to the model risk governance process, including its registration in Nubank's model inventory.

For all other inquiries, employees use a centralized risk management platform, which features an intelligent routing system that forwards requests to the appropriate teams based on the inherent risk level, calculated according to pre-defined criteria.

Part II. Mapping digital governance domains

Interconnected risks are the new normal.

Gone are the days of digital risks being exclusively siloed — where cyber risks, for example, landed squarely with the cyber or IT department and privacy risks were addressed mainly by the legal department and seen through the lens of regulatory compliance.

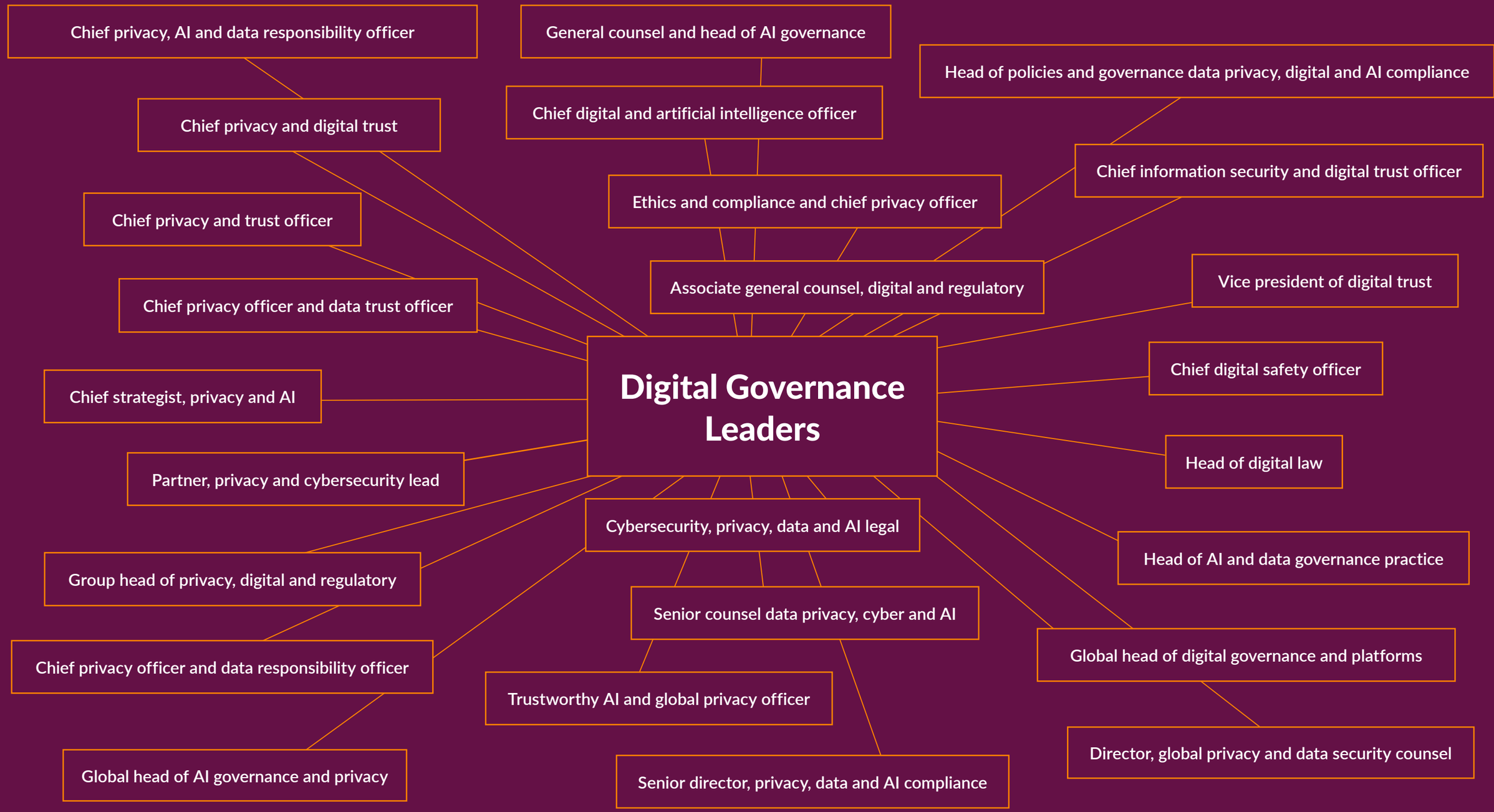
Continuous innovation in the digital environment, whether it be the proliferation of Internet of Things devices or the rise of intuitive generative and agentic AI models, has shifted the way organizations perceive and operationalize their risk mitigation approaches. Today's risks span multiple domains and siloed approaches may prove to be fundamentally inadequate in addressing the new, interconnected and complex digital risk environment.

Modern organizational governance architectures have responded to this by moving towards more integrated and aligned functions, bringing together multiple domains and disciplines. For instance, customer relationship management architectures may contain tools used for customer acquisition, ongoing customer relationship management and managing rights requests and marketing consents. AI governance architectures may contain tools used for managing AI use cases, implementing appropriate controls and aligning with regulatory and other compliance requirements.

> **Today's leaders in digital governance draw on the combined strengths of privacy, cyber, information governance, AI, data ethics, and even ESG-driven data sustainability. Grounded in law, risk, technology, and human impact, they bring a multi-dimensional lens to questions of fairness, accountability and trust. We need architects of digital trust, professionals who can embed these considerations into the core of how we design, deploy and scale data solutions. In the life sciences industry, this isn't just a responsibility; it's a strategic and survival imperative.**
>
> **João Barreiro**
> CIPP/E, CIPP/US, chief privacy and data ethics officer, BeOne Medicines

What does a more integrated and aligned digital governance strategy look like? How are organizations maturing their approach to get there?

It is rare to find organizations with a neat, defined, aligned and long-standing digital governance function. Domain-specific governance functions, while historically robust, can be challenging to adapt as organizations pursue more integrated approaches. As a result, many organizations have embedded the primary duties of a broader and more holistically defined function of digital governance within their preexisting AI, privacy and cyber departments. This trend is shown in the growth of job titles to include additional domains.

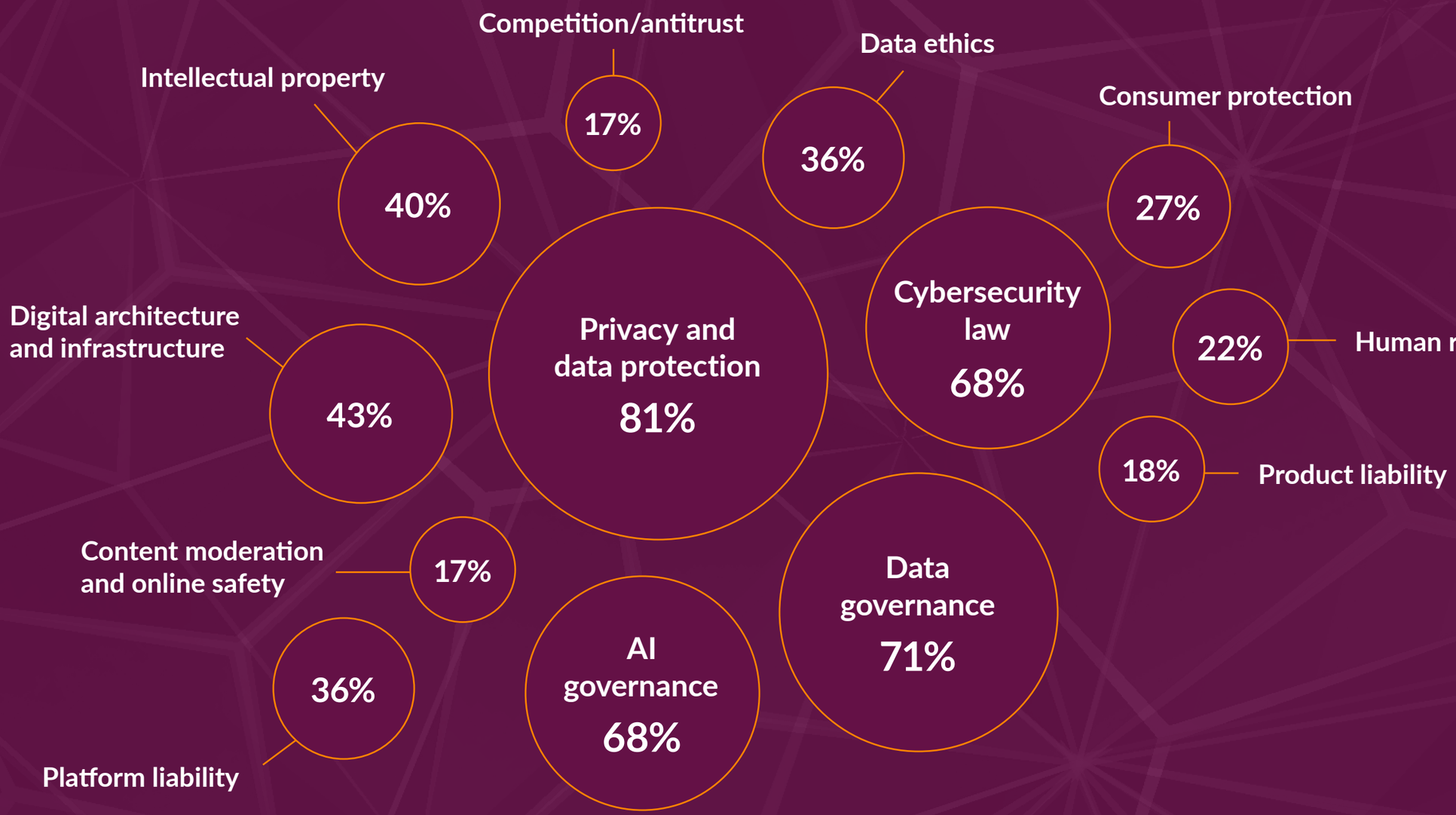

Digital Governance Leaders
Chief privacy, AI and data responsibility officer
Chief privacy and digital trust
Chief privacy and trust officer
Chief privacy officer and data trust officer
Chief strategist, privacy and AI
Partner, privacy and cybersecurity lead
Group head of privacy, digital and regulatory
Chief privacy officer and data responsibility officer
Global head of AI governance and privacy
General counsel and head of AI governance
Chief digital and artificial intelligence officer
Ethics and compliance and chief privacy officer
Associate general counsel, digital and regulatory
Cybersecurity, privacy, data and AI legal
Senior counsel data privacy, cyber and AI
Trustworthy AI and global privacy officer
Senior director, privacy, data and AI compliance
Head of policies and governance data privacy, digital and AI compliance
Chief information security and digital trust officer
Vice president of digital trust
Chief digital safety officer
Head of digital law
Head of AI and data governance practice
Global head of digital governance and platforms
Director, global privacy and data security counsel

Broadly speaking, organizational digital governance can encompass any combination of digital risk domains, such as privacy and data protection, AI governance, cybersecurity, content moderation, online safety, platform liability, digital accessibility, data governance and ethics. Depending on the organization, digital governance may be "synonymous with enterprise risk governance" or it may be "much more discrete as a part of broader enterprise risk governance efforts," as discussed in the IAPP 2024 Organizational Digital Governance Report.

Depending on an organization's product, service and geographic footprint, different governance domains will be included in what they might term their broader digital governance approach. Some domains will be more prevalent across organizations than others, given their horizontal and all-economy relevance, such as privacy and data governance, whereas others may be more specific to individual organizations based on their footprint, such as platform liability and consumer protection. To this end, we asked respondents to enumerate the domains included in their organization's overall digital governance approach.



The evolving web of digital governance



Note: % denotes proportion of respondent's organizations that include selected domain in the digital governance approach.

With 81% of respondents citing it, privacy/data protection emerges as the most commonly integrated domain in digital governance approaches. Data governance closely follows at 71%, and both AI governance and cybersecurity are tied for third at 68%. These domains are closely related, so it is not necessarily surprising to see the majority of organizations include them in their approach. Interestingly, the domains toward the bottom of the list — content moderation/online safety and competition/antitrust — were still both selected by 17% of respondents, suggesting these concerns are likely more relevant for specific players in the digital ecosystem.

Overall, the average number of domains included in an organization's digital governance approach is just over five. More than 50% of respondents have at least three domains included in their digital governance approach, with almost 30% reporting at least five domains are included.

> **The laws affecting digital governance are like an ever-evolving glacier, which moves more slowly than the technology they are trying to regulate but is never static. For those who need to manage the implications of this evolving legal framework, this means staying super-alert to all the changes taking place and being prepared to make and alter decisions as they go along. In practice, this requires understanding how existing laws need to be correctly applied to novel situations and also learning how new laws affect the development and deployment of technologies like AI and biometrics. More than ever, digital governance professionals need to be able to take a view on business-critical and strategic issues in the absence of perfect information.**
>
> Eduardo Ustaran
> AIGP, CIPP/E, partner, Hogan Lovells

Part III. Maturing digital governance functions

Digital governance approaches are forming.

Key to supporting an innovative mindset from within the governance function is also the need for the organization to mature its approach to governance. While technologies may have been rapidly adopted by organizations, the maturity of digital governance within organizations may slow its loftier digital ambitions.

Traditional governance models that operate in silo were largely designed for an analog world, one less connected and experiencing fewer systemic changes. In some cases, the governance gap can be vast, a chasm between an organization's digital footprint and the underlying governance framework, preventing it from effectively realizing opportunities.

A governance approach that is completely reactive can hinder an organization, with a "fix it when it breaks" mentality, leaving an organization vulnerable and not primed to take risks and seize opportunities. Instead, a proactive approach embedded within a continuously improving digital governance framework may support the organization to not only mitigate risks but unlock unprecedented value and competitive advantage.

This year's survey sought to understand the maturity of organizations' approach to digital governance.

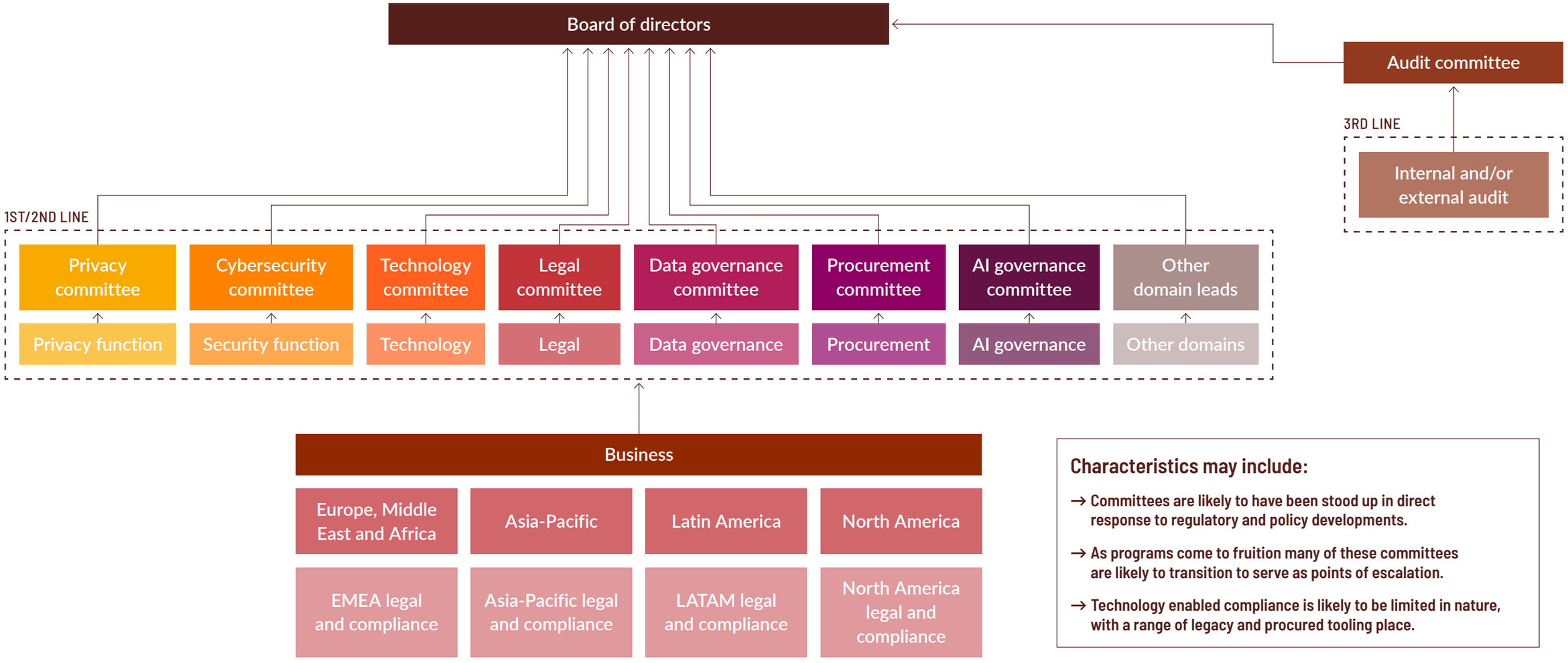
→ **Analog** — An analog model for an organization seeks to implement digital governance within and throughout individual subdomains without a defined or coherent approach to digital governance.

→ **Augmented** — 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.

→ **Aligned** — An aligned model has streamlined the processes and structures into a more singularly defined and framed approach to digital governance.

Analog governance

This model implements digital governance through existing structures without a defined or cohered approach.



Characteristics may include:

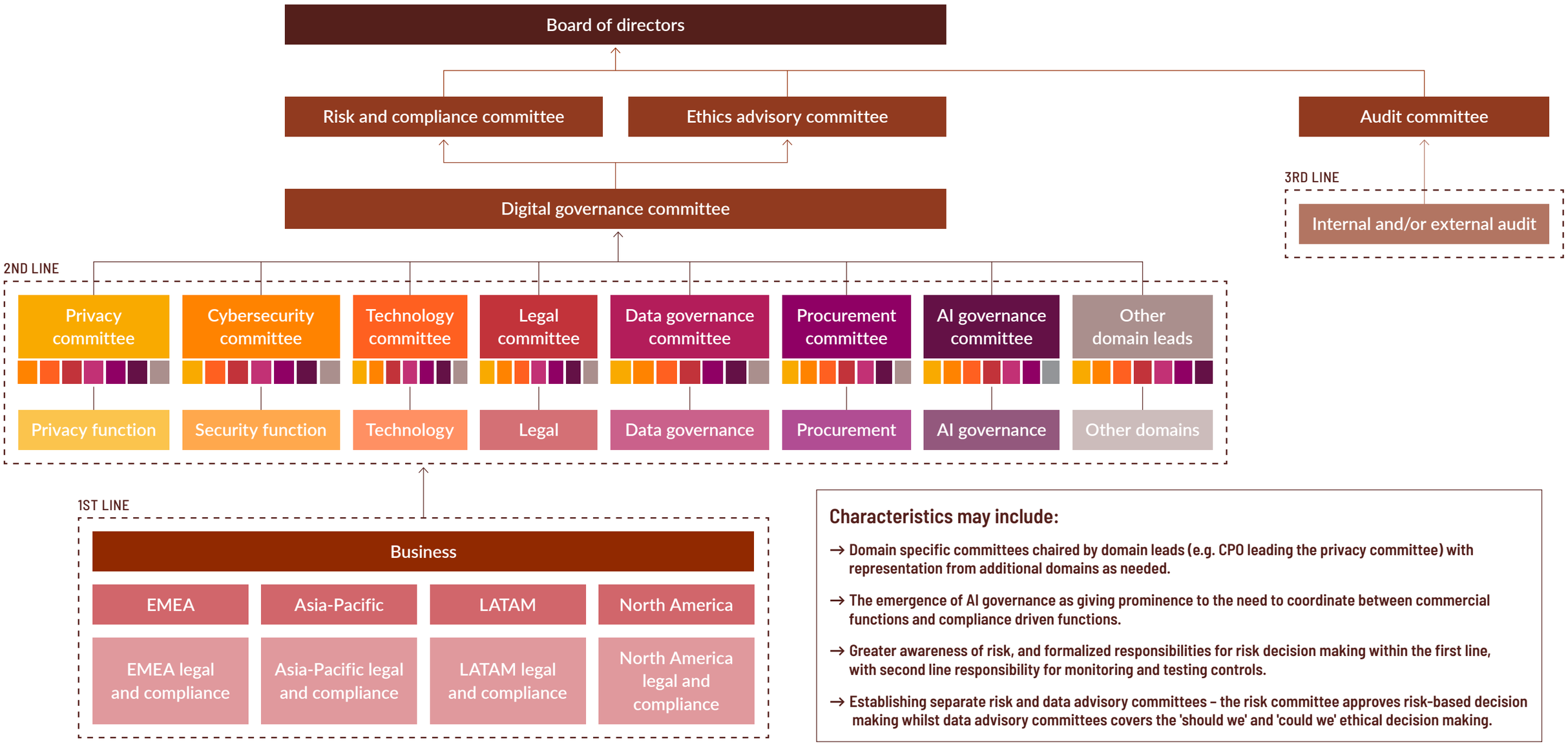
→ Committees are likely to have been stood up in direct response to regulatory and policy developments.

→ As programs come to fruition many of these committees are likely to transition to serve as points of escalation.

→ Technology enabled compliance is likely to be limited in nature, with a range of legacy and procured tooling place.

Augmented governance

This digital governance model implements interdisciplinary processes and structures in a defined approach.



Characteristics may include:

- → Domain specific committees chaired by domain leads (e.g. CPO leading the privacy committee) with representation from additional domains as needed.
- → The emergence of AI governance as giving prominence to the need to coordinate between commercial functions and compliance driven functions.
- → Greater awareness of risk, and formalized responsibilities for risk decision making within the first line, with second line responsibility for monitoring and testing controls.
- → Establishing separate risk and data advisory committees – the risk committee approves risk-based decision making whilst data advisory committees covers the 'should we' and 'could we' ethical decision making.

Aligned governance

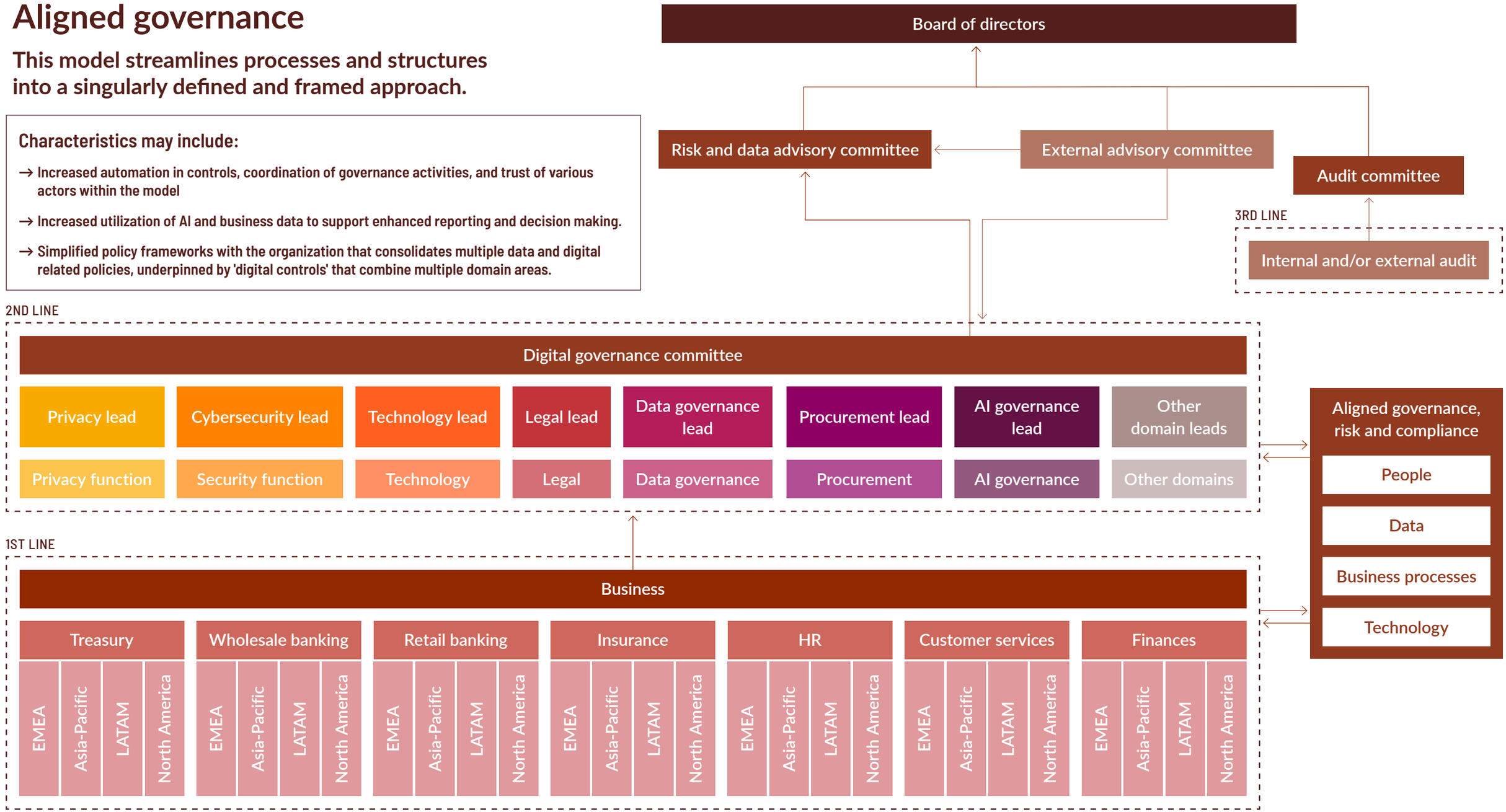
This model streamlines processes and structures into a singularly defined and framed approach.

Characteristics may include:

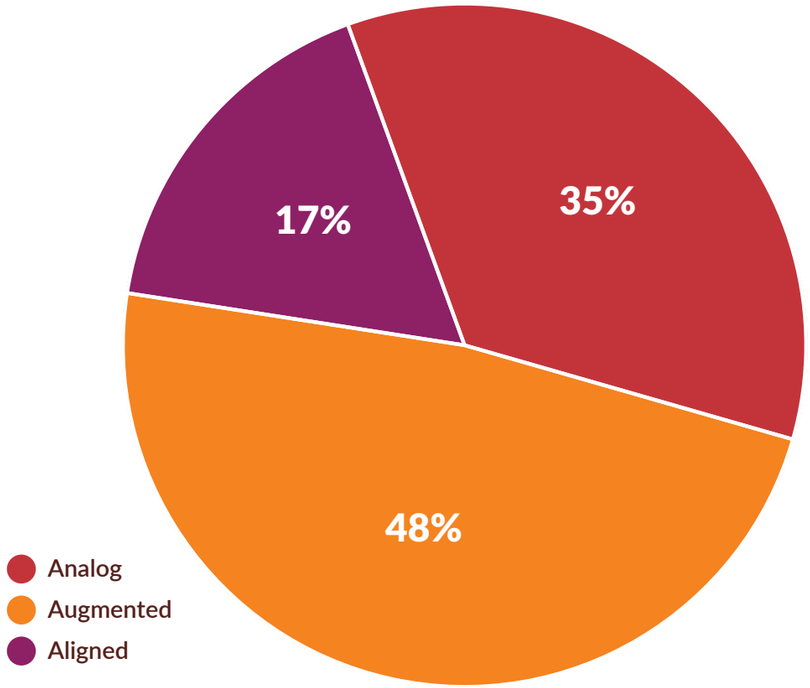
→ Increased automation in controls, coordination of governance activities, and trust of various actors within the model

→ Increased utilization of AI and business data to support enhanced reporting and decision making.

→ Simplified policy frameworks with the organization that consolidates multiple data and digital related policies, underpinned by 'digital controls' that combine multiple domain areas.



Maturity of digital governance, overall



Of organizations whose annual revenue is smallest — less than USD100 million — 41% have analog digital governance models, while, significantly, only 16% of the largest organizations by annual revenue — USD60 billion or more — have the same structure. Overall, the larger the organization's revenue is, the more likely they are to have either an augmented or aligned maturity model. Similarly, the likelihood of an organization having an analog maturity model trends downward as revenue increases.

Maturity of digital governance, by annual revenue (USD)

	Overall	Small (Under 100M)	Medium (101M-999M)	Large (Greater than 1B)
Analog	35%	41%	41%	29%
Augmented	48%	39%	42%	56%
Aligned	17%	20%	17%	15%

Maturity of digital governance, by sector

	Overall	Banking and insurance	Technologies and telecoms	Education and nonprofit	Business services	Consumer goods, services and retail	Government	Life sciences and health care	Legal	Manufacturing	Other
Analog	35%	34%	31%	52%	23%	52%	38%	39%	23%	33%	32%
Augmented	48%	53%	40%	42%	38%	43%	55%	47%	41%	56%	50%
Aligned	17%	13%	29%	6%	38%	5%	7%	13%	36%	11%	18%

The type of maturity model is also affected by the industry sector. Organizations in both the education/nonprofit and the consumer goods sectors were particularly more likely than average to identify having an analog maturity model. Education and nonprofit organizations may not be as exposed to many of the risks that come with a large digital risk profile, like organizations in the technology and telecommunications industry are.

To that point, technology and telecommunications organizations, as well as business services organizations, were significantly more likely to have implemented an aligned maturity model, at 29% and 38%, respectively, compared to the overall average of 17%.



The role of digital governance committees for innovation

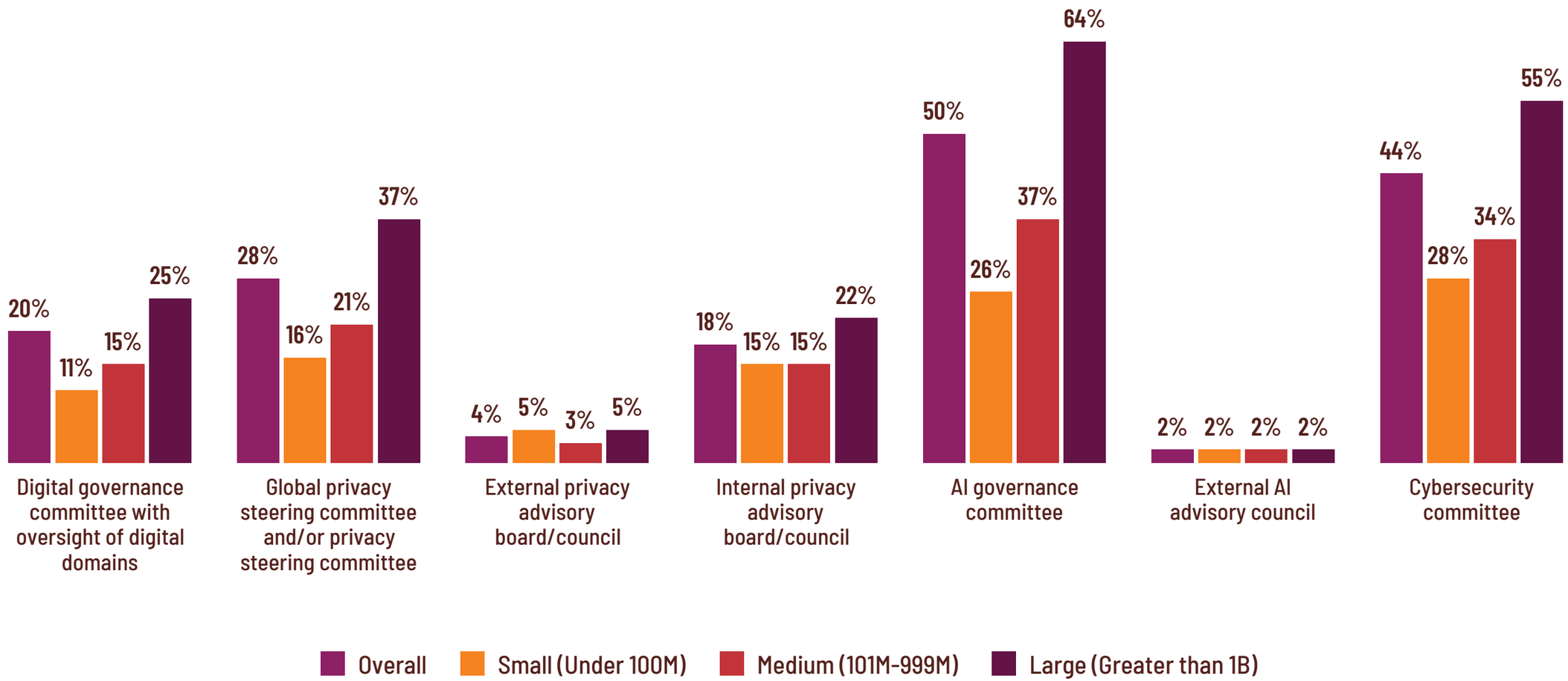
The establishment and effective workings of a digital governance committee with a remit of defining and actioning digital responsibility can be a driver of innovation within organizations. Those committees, especially those with senior representation, may open lines of communication and escalate to key decision makers within the organization, raise awareness and drive investment.

Digital governance committees are not solely for large organizations with the luxury of having numerous human resources to bring together. Several small and medium organizations reported their organization designated such committees. Unsurprisingly, given its strategic importance for many organizations, AI governance committees were among the most popular types of governance committees appointed.

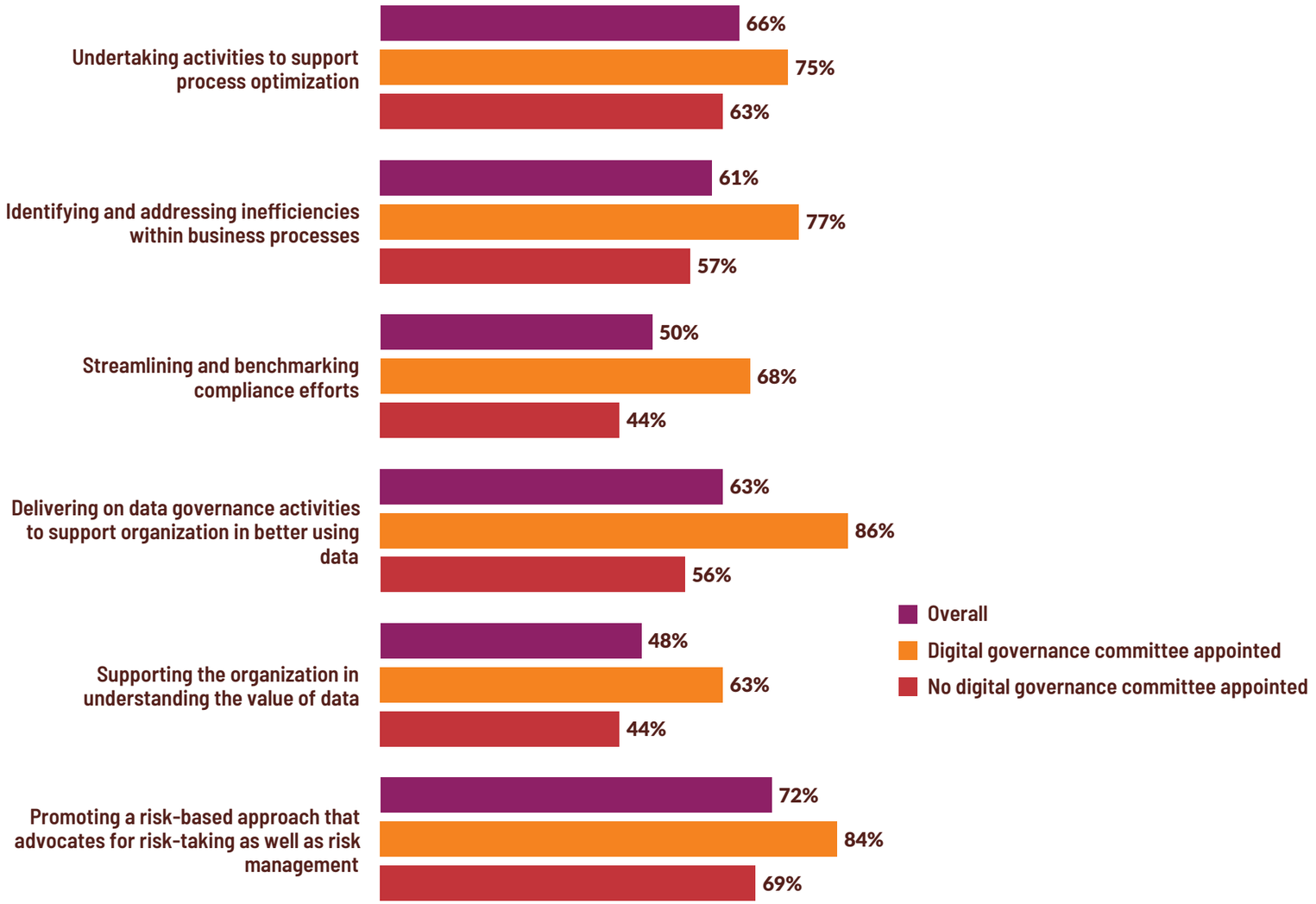
These are likely associated with AI governance programs with organizations working on meeting the requirements of various AI frameworks and regulations as well as supporting strategic pushes into AI deployment within the organization more broadly. As these programs come to fruition, it will remain to be seen whether these committees will evolve into digital governance committees, be repurposed to tackle another cross-cutting governance issue or be wound down completely.

> **Autodesk prioritizes ethical, secure, and transparent AI development, deployment, and use. In order to foster trust and understanding, we've introduced resources such as Transparency Cards, Autodesk's Trusted AI Practices eBook, and dedicated Trust Center content. These efforts are supported by ongoing collaboration across our legal, trust, sales and customer support teams — ensuring continuous improvement and reinforcing the value and trustworthiness of Autodesk AI.**
>
> **Alexandra Ross**
> CIPP/E, CIPP/US, CIPM, CIPT, FIP, PLS, senior director, senior data protection, use and ethics counsel, Autodesk

Established committees within the organization, by annual revenue (USD)



Innovation activities undertaken by organizations that appoint digital governance committees



Responses to this year's survey showed how organizations with digital governance committees in place were more likely, sometimes significantly so, to have indicated they undertake activities geared towards digital innovation compared to the overall average.

While the existence of a digital governance committee may not be a requirement of undertaking innovation, organizations may find such an appointment useful to consider as they seek to mature their organization's approach to digital governance.

> **In 2025, digital governance has become a board-level issue. Clients are no longer treating it as just a privacy or compliance concern, but as a strategic framework integrating data ethics, cybersecurity, AI governance, and business continuity. Organizations that embed legal and risk expertise early in digital initiatives not only reduce exposure but also unlock value — especially in cross-border operations, mergers and acquisitions, and AI deployment. Governance maturity is now a market differentiator.**
>
> **Diego Fernández**
> partner, Marval O´Farrell & Mairal



Part IV. Regulatory risk or reward?

Good digital governance matters regardless of the external regulatory environment.

The pace of — and the increasing uncertainty surrounding — digital regulation has posed complex challenges for those in the digital governance space. One such challenge is regulation.

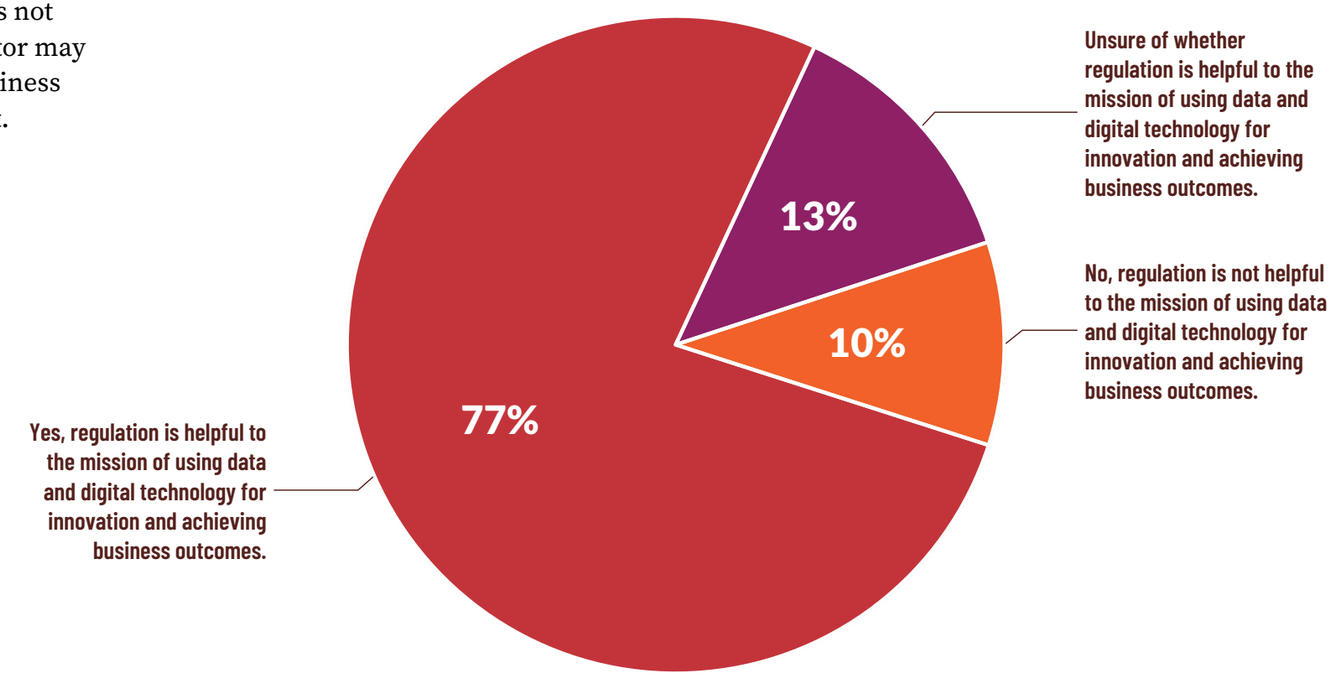
Many organizations have invested considerable time and resources into their compliance efforts. But good digital governance goes beyond compliance and is, instead, the foundation of how an organization achieves its business objectives sustainably, responsibly and ethically. The threat of deregulation looms large; while it may change the external regulatory environment, it may do little to change consumer expectations of control and the financial, reputational and operational impacts should an organization get it wrong.

Thus, talk of deregulation begs the question: how are organizations perceiving the current digital regulatory environment? Overall, nearly 8 out of 10 organizations believe regulation is helpful to the mission of using data and digital technology for innovation-achieving business outcomes.

This perception varies slightly depending on industry sector. For example, organizations in the consumer goods/retail sector were significantly less likely to view digital regulation as helpful for innovation and business growth, at 57%. These organizations were also significantly more likely to be unsure, at 29%. However, only 10% of those in the consumer goods/retail sector would not continue to invest in digital governance activities if it were deregulated.

Overall, this suggests the consumer goods/retail sector may still be in the early stages of developing digital governance approaches and is not yet at the stage where the sector may recognize innovation and business growth from their investment.

Overall, nearly 8 out of 10 organizations believe regulation is helpful to the mission of using data and digital technology for innovation-achieving business outcomes.



Do you view regulation as helpful to the mission of using data and digital technology for innovation and achieving business outcomes? By sector

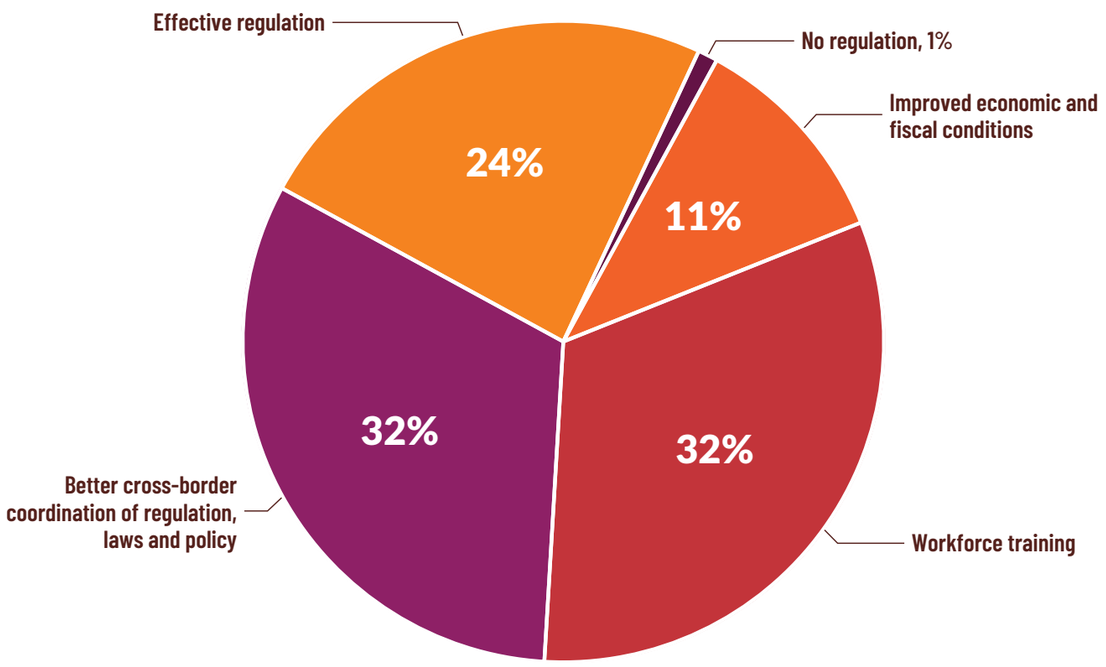
	Overall	Banking and insurance	Technologies and telecoms	Education and nonprofit	Business services	Consumer goods, services and retail	Government	Life sciences and health care	Legal	Manufacturing	Other
Yes	77%	81%	82%	74%	77%	57%	79%	87%	68%	78%	76%
No	10%	12%	4%	13%	15%	14%	7%	5%	18%	0%	11%
Unsure	13%	7%	13%	13%	8%	29%	14%	8%	14%	22%	13%

The perception of digital regulation also varies by continent. Over 9 out of 10 respondents from Asia and Oceania, for example, view regulation as helpful for innovation and business growth, compared to just under 8 out of 10 overall.

Do you view regulation as helpful to the mission of using data and digital technology for innovation and achieving business outcomes? By continent

	Overall	North America	Europe	Asia	South America	Africa	Oceania
Yes	77%	75%	77%	91%	86%	83%	93%
No	10%	10%	13%	5%	0%	0%	0%
Unsure	13%	16%	10%	5%	14%	17%	7%

Most likely ways to help improve digital innovation, overall



In terms of improving digital innovation, 1 in 3 believes workforce training — and a further 1 in 3 believes better cross-border coordination of regulation — would be more effective than no regulation, selected by only 1% of respondents.

Organizations vary on what they believe would improve digital innovation when broken down by sector. For instance, though 82% of those in the tech/telecommunications sector reported digital regulation is helpful for innovation and business growth, they were significantly less likely to report that effective regulation would improve digital innovation — only 9% compared to 24% overall.

Half of respondents in the government sector indicated workforce training would improve digital innovation, compared to only 32% overall. These respondents were also significantly less likely to indicate that better cross-border coordination of regulation, laws and policy would improve digital innovation —14% compared to 32% overall. Those in the government sector could potentially benefit considerably from investments in training and preparing their workforce for digital innovation.

Most likely ways to improve digital innovation, by continent

	Overall	North America	Europe	Asia	South America	Africa	Oceania
Training of workforce	32%	31%	32%	32%	43%	17%	40%
Better cross-border coordination of regulation, laws and policy	32%	30%	37%	32%	14%	33%	33%
Effective regulation	24%	28%	18%	9%	29%	17%	13%
Improved economic and fiscal conditions	11%	10%	10%	27%	14%	33%	13%
No regulation	1%	0%	3%	0%	0%	0%	0%

There are two particularly interesting trends by region. First, North American respondents were significantly more likely, at 28%, to report effective regulation as a way to improve digital innovation, compared to 24% overall. Perhaps North American organizations would feel more certain in their innovation activities if they had regulations and policies to guide their approach.

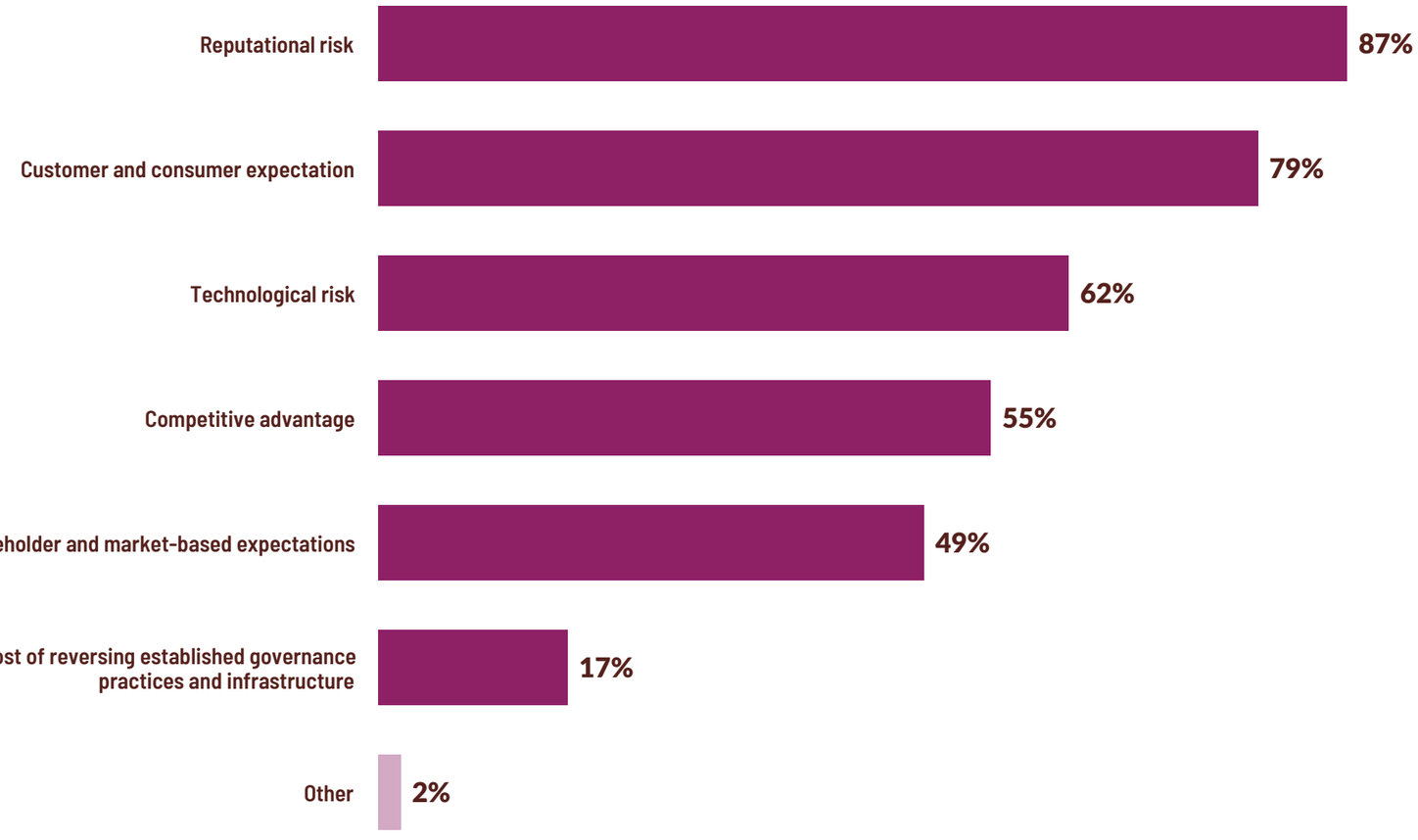
Second, more than one quarter of respondents from Asia indicated that improved economic and fiscal conditions would help improve digital innovation, compared to just 11% overall.

Organizations are broadening their perspectives and framing digital governance not as a cost center but as a strategic function that supports risk management and better decision making. Theoretically, while deregulation may be considered to foster innovation through reducing compliance burdens, it may ultimately come with hidden costs, with a greater onus on existing governance functions to tackle bad conduct.

Even if faced with a deregulated external environment, many organizations recognize governance activities as more than just a response to regulation and compliance assurance. Of respondents, 70% believed their organization would continue to invest in and deliver on governance activities even if deregulation were to occur. Of those that would continue governance activities, 56% stated that while governance activities would continue, they would do so in different ways. Respondents also identified a variety of reasons as to why their organization would continue to deliver on governance.

Of respondents, 70% believed their organization would continue to invest in and deliver on governance activities even if deregulation were to occur. Of those that would continue governance activities, 56% stated that while governance activities would continue, they would do so in different ways.

Reasons for continuing to deliver on digital governance where there is deregulation, overall



Many of these factors are intrinsically linked to an organization's ability to grow, compete and innovate. Organizations that embrace a professionalized and well-governed way of managing and taking risks when it comes to digital technologies may gain a significant competitive advantage while simultaneously recognizing new efficiencies.

Case Study - HERE Technologies - Cross-functional collaboration is foundational for sustainable growth and trust

HERE Technologies specializes in location data and technology, providing high-precision maps, real-time navigation services, and geospatial application programming interfaces that power intelligent mobility across industries. As AI and automation reshape transportation and mobility, HERE plays a critical role in delivering location services.

At the intersection of technology, regulation and digital business transformation, HERE has a governance framework in place to address the growing complexity of legal, ethical and operational risks in an AI-driven world.

Emerging regulations, such as the EU AI Act, Cyber Resilience Act and Data Act, are fundamentally changing how organizations must handle AI, data, cybersecurity and digital products. These frameworks extend legal responsibilities across the entire digital value chain, introducing heightened obligations around safety, explainability, liability and data sharing.

Recognizing the increasing interdependence between innovation and compliance, HERE has shaped its governance strategy to address risk not only as a legal requirement, but as a foundation for sustainable growth and trust.

The company's digital governance model is founded on strong cross-functional collaboration, bringing together expertise from legal, compliance, product development, engineering and business teams in a shared commitment to responsible innovation. A key component of this collaboration is the integration of strategic legal insights that align digital transformation efforts with an evolving regulatory landscape.

With broad visibility into digital priorities and deep subject matter expertise, the digital legal function plays a pivotal role in shaping consistent, forward-looking governance, particularly in areas like AI, privacy, cybersecurity and data governance. This approach embeds compliance into the earliest stages of product development and equips the organization to respond proactively and confidently to regulatory change.

HERE's proactive approach to digital governance is intended to differentiate it in an increasingly regulated market. By anticipating legal developments and embedding structured safeguards into its operations, the organization can build stronger, trust-based relationships with customers and partners, particularly in highly regulated industries, such as automotive and mobility. This approach supports faster delivery of AI-powered solutions while upholding high standards of transparency, safety and accountability.

Part V. Governance driving innovation

An effective digital governance approach may help accelerate — not hinder — innovation within an organization.

An increasingly outdated view of governance is that it is focused on risk management and mitigation, regulatory compliance and exerting control; this perspective often treats governance as a brake to slow down or stop initiatives to create, innovate and adopt digital technologies. Innovation is now a critical driver for organizations to remain competitive, resilient and sustainable. The rapid pace of change, market disruptions and unforeseen events all require a novel approach. Those that fail to innovate risk being left behind, chasing shadows and, in the worst case, disappearing altogether.

The apparent tension and disconnect between the traditional rigid role played by governance versus the fluid, chaotic approach of innovation is worth tackling. How are governance functions tackling this today? Governance functions can be tasked with fostering innovation — or can they? If so, how are they supporting innovation?

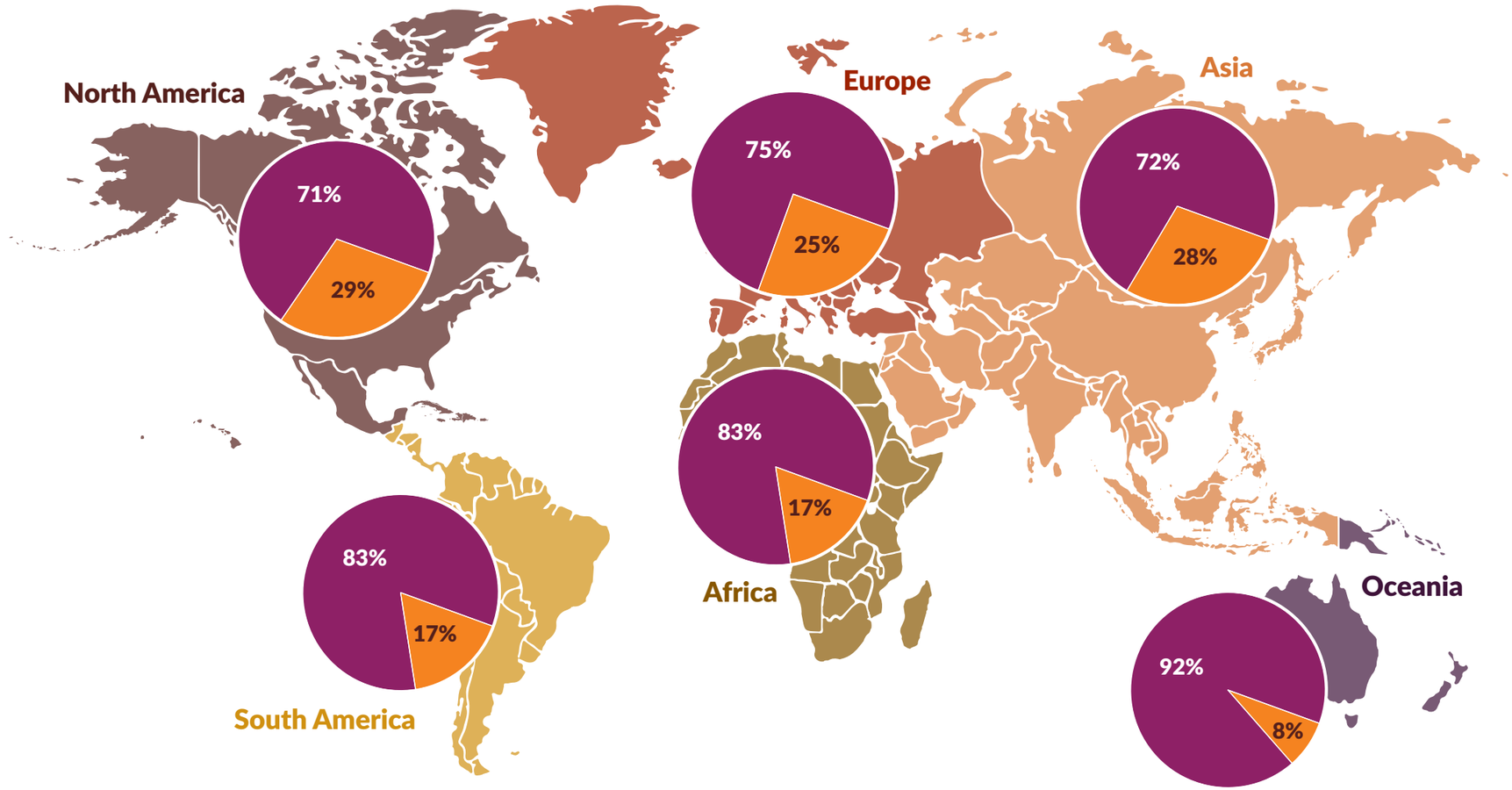
Of those who could identify their organization's approach, 74% of respondents identified that their governance functions are tasked with supporting technological innovation and/or business growth.

Tasked with innovation

Of those who could identify their organization's approach, 74% of respondents identified that their governance functions are tasked with supporting technological innovation and/or business growth.

Those more confident in their organization's ability to stay compliant were more likely to indicate that their governance functions are being tasked with technological innovation or business growth when compared to those not at all confident. Significantly, only 20% of those who identified as not at all confident in their organizations' compliance ability also reported being tasked with technical innovation and business growth, compared to 69% of those who identified as strongly confident in their organizations' compliance ability. Strong, confident governance functions are being leveraged for growth and innovation.

Contribution of governance functions globally to innovation and business growth, by continent



Is your organization's governance function(s) being tasked with work that is focused on technological innovation or business growth?

Yes

No

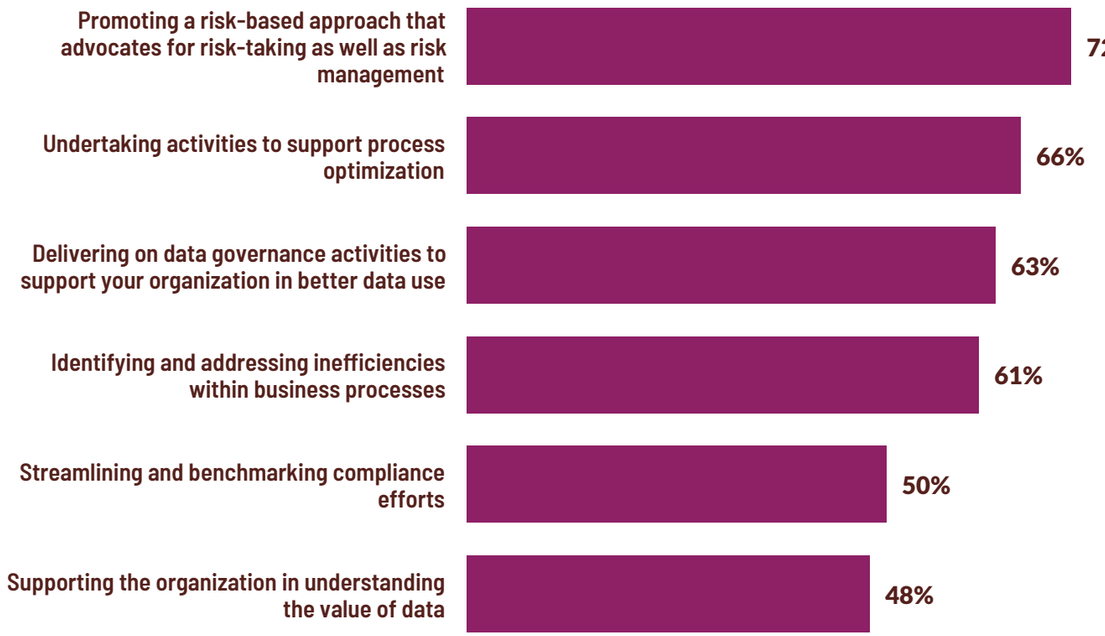
Spotlight on examples of digital governance practices driving innovation

Identifying and addressing inefficiencies within business processes — proactively discovering and fixing redundant steps, bottlenecks, or misallocated resources within an organization to improve productivity and, ideally, reduce costs	**Process optimization** — Systematically improving existing business processes to make them more efficient and effective to enhance overall organizational performance	**Streamlining and benchmarking compliance efforts** — simplifying and standardizing compliance-related activities, as well as comparing an organization's compliance performance against industry best practices and regulatory requirements to identify areas for improvement
Examples inlcude:	**Examples inlcude:**	**Examples inlcude:**
• Simplifying overlapping risk assessments. Integrate domain specific risk assessments — e.g., privacy impact assessments, AI risk assessments, cyber risk assessments — into a single assessment portal, with questions based on risk, in scope domains and business priorities. • Streamlining AI model retraining and maintenance cycles. Assess the process of retraining and updating AI models and identify inefficiencies — e.g., long validation processes, poor data identification and governance — and implement machine learning operations practices to automate data drift detection. • Refining data retention policies. Analyze current data retention practices against legal and business requirements, identifying instances of over-retention of personal data, and implement automated deletion or anonymization schedules to reduce unnecessary data accumulation.	• Automating data subject access requests. Integrate a workflow automation tool that automatically routes DSARs to the relevant data stewards, tracks actions and deadlines and generates prepopulated response templates. • Implementing privacy-by-design checklists in SDLC. Integrate more automated privacy impact assessments or data protection impact assessments directly into the software development life cycle that flags potential privacy risks in early design stages, prompting developers to build in privacy controls from the outset. • Centralizing consent management. Optimize the process of collecting and manage consent by deploying a universal consent management platform across the digital footprint — e.g., websites and apps — that allows self-service management of preferences and integrates with backend systems to consistently honor preferences.	• Streamlining and benchmarking compliance so it is proportionate to peers and the risk environment. Scarce resources are effectively prioritized to help the organization meet proportionate compliance needs while also being available for growth activities. • Productizing compliance for merger and acquisition activities. Organizations that grow through acquisition activity may require their compliance functions to rapidly roll out compliance in their new businesses. Streamlining compliance efforts and turning them into a product may enable rapid rollout and a scalable solution that enables digital governance efforts to be an opportunity rather than a cost center. • Maintaining a competitive and comparative advantage. Organizations with a demonstrably better approach and delivery of digital governance and compliance requirements than competitors may present opportunities to leverage trust in the B2B and B2C marketplace.

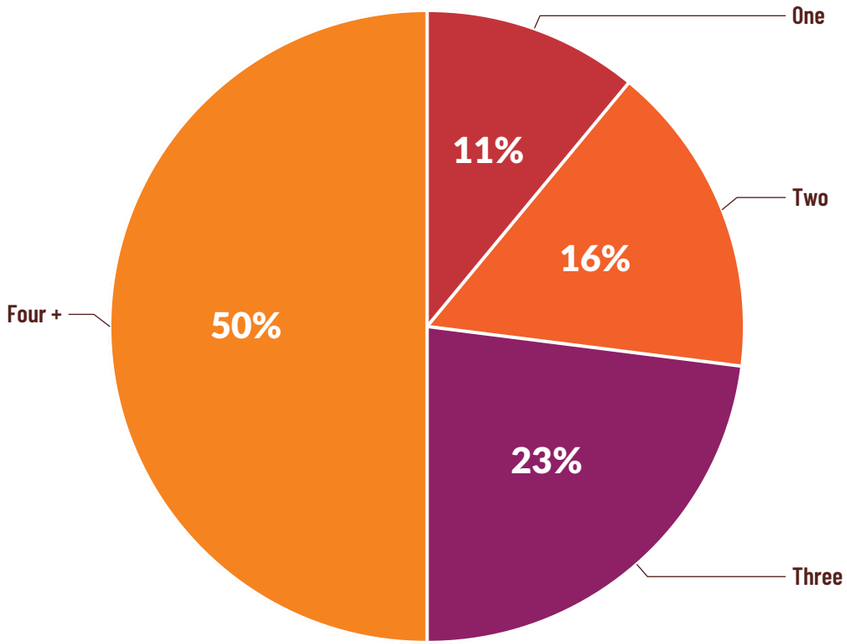
Delivering on data governance activities to support your organization in better data use — improving policies, standards and processes to ensure the quality, integrity, security, usability and availability of data across an organization	**Supporting the organization in understanding the value of data** — communicating the strategic importance of data, promoting a data-driven culture and enabling employees to use data for improved decision-making and innovation	**Promoting a risk-based approach that advocates for risk-taking as well as risk management** — alongside identifying, assessing and mitigating risks, advocate and provide the framework to seize opportunities that involve a calculated level of risk
Examples inlcude:	**Examples inlcude:**	**Examples inlcude:**
• Improving data catalogs with privacy and AI governance specific metadata. This means updating the data catalog so it includes reference to more specific metadata, such as retention periods, legal basis of processing, data lineage and data ownership. • Developing a first-line data stewardship program as part of first-line digital governance responsibilities. Appointing data stewards with responsibility across digital governance domains for data within their first-line business unit can bridge the gap between data use and digital governance considerations. • Integrating synthetic data generation to preserve data utility and privacy considerations. Implement tools and processes that generate synthetic data that mimics the statistical properties and patterns of personal data and integrate these into existing data request processes — e.g., where real personal data would usually be requested for AI projects.	• Quantifying the return on investment into digital governance. Enhance existing business cases to illustrate the long-term strategic advantages gained from investing into maturing the organization's digital governance approach. • Enhancing risk assessments through risk quantification. Build quantitative risk models with a focus on data use — e.g., operational inefficiencies due to poor data quality, the opportunity cost of poor data use, or the impact of data breach. • Integrating digital governance objectives into performance reviews. Work with human resources and department heads to integrate specific, measurable, achievable, relevant, and time-bound, also known as SMART, objectives to cover digital governance into annual performance reviews of key roles.	• Implementing an enhanced fast track risk assessment lane for strategically important projects. Those that seize market opportunities or drive innovation are rapidly risk assessed and approved. The fast lane avoids delays or bottlenecks in existing risk review processes and incentivizes strategically important ideas that involve calculated risk. • Establishing an organizational approach to regulatory arbitrage. Taking advantage of differences in regulations or laws may have broader implications for the industry and come with ethical considerations. However, an organization that has an agreed upon approach to taking legal risk through regulatory entrepreneurship may be able to win the race to strategically position itself ahead of competitors. • Creating an M&A digital governance playbook. For an organization that regularly undertakes M&A activity, developing a playbook that rapidly rolls out a digital governance framework post-M&A may encourage faster and more successful integration.

The chain reaction of innovation

Types of innovation activities undertaken by governance functions



Number of innovation activities undertaken by governance functions, overall



Combinations of innovation activites

Innovation-supporting activities do not take place in isolation. For example, of those that undertake activities to identify and address inefficiencies within business processes, 77% also work on process optimization, 57% on streamlining and benchmarking compliance efforts, and 79% on promoting a risk-based approach.

For those performing each innovation activity we asked about, at least 50% — and a far greater percentage in many cases— identified performing every other innovation activity polled. In other words, those being tasked with innovation are more than likely driving it on multiple different fronts across the organization. This also suggests that progress in one area can have compounding effects across the organization, potentially sparking advancements and improvements in other areas.

	Undertaking activities to support process optimization	Identifying and addressing inefficiencies within business processes	Streamlining and benchmarking compliance efforts	Delivering on data governance activities to support your organization in better data use	Supporting the organization in understanding the value of data	Promoting a risk-based approach that advocates for risk-taking as well as risk management
Undertaking activities to support process optimization		77%	75%	70%	70%	68%
Identifying and addressing inefficiencies within business processes	71%		71%	66%	68%	66%
Streamlining and benchmarking compliance efforts	56%	57%		53%	52%	56%
Delivering on data governance activities to support your organization in better data use	66%	68%	67%		81%	67%
Supporting the organization in understanding the value of data	51%	54%	51%	62%		52%
Promoting a risk-based approach that advocates for risk-taking as well as risk management	75%	79%	82%	78%	78%	

Case Study - GlobalLogic x Lytx - Complex digital risks drive adoption of aligned digital governance

Lytx is a provider of AI-powered video telematics, analytics, safety and productivity solutions for commercial and public sectors. Using the world's largest driving database of its kind, along with proprietary machine vision and AI technology, the company helps protect and connect thousands of fleets and more than 1 million drivers worldwide. The application of MV+AI means digital technologies are altering the organizational risk environment, introducing complex considerations around data privacy, algorithmic bias, ethical implications and security.

In Lytx's role in video safety and telematics, we are proactively adapting to a dynamic regulatory landscape, including new frameworks like the EU AI Act. The importance of addressing increasingly complex digital risks influenced digital governance strategies. To help propel efforts in AI governance, the company collaborated with GlobalLogic to focus on designing and implementing a robust governance framework, so responsible AI is integrated throughout the entire model lifecycle, from initial concept to decommissioning.

Lytx's digital governance structure involves multiple domains interacting to create a cohesive approach, including product, technology, compliance, legal and information security. This team sport approach enables tight collaboration between these functions. The AI Governance Council brings together cross-functional leaders to embed safety and ethics by design. GlobalLogic supported this by integrating regulatory compliance, technical understanding, privacy protection, and strategic business objectives into a unified approach. This has led to a more coordinated approach to AI governance, transforming previously fragmented processes into an embedded governance strategy.

The evolving regulatory landscape has shaped Lytx's governance, prompting ethical development practices that stay ahead of regulation. The company's governance framework now aligns with leading standards like the EU AI Act and the National Institute of Standards and Technology AI Risk Management Framework, with ongoing adaptation to new regulations and emerging AI risks, such as bias, fairness, security and data privacy. These elements are rigorously evaluated through an AI risk impact assessment process for every model. Human oversight is also a critical component, ensuring AI is never fully autonomous in high-risk scenarios.

Lytx's investment in and approach to digital governance has demonstrably supported business growth, transforming a compliance challenge into a competitive advantage.

The importance of better leadership buy-in

Despite the efforts of digital governance professionals to drive meaningful change in their organization, 42% of respondents identified that senior leaders do not understand or appreciate how their role can enable innovation and growth.

This could be for a variety of reasons, including lack of leadership buy-in related to governance activities, siloed leadership structures or belief that governance is the antithesis to innovation.

Employees who find themselves in this situation may find success in demonstrating that investing in digital governance structures will not only help innovate the organization's overall governance, but could facilitate direct positive impacts on first-line business activities.

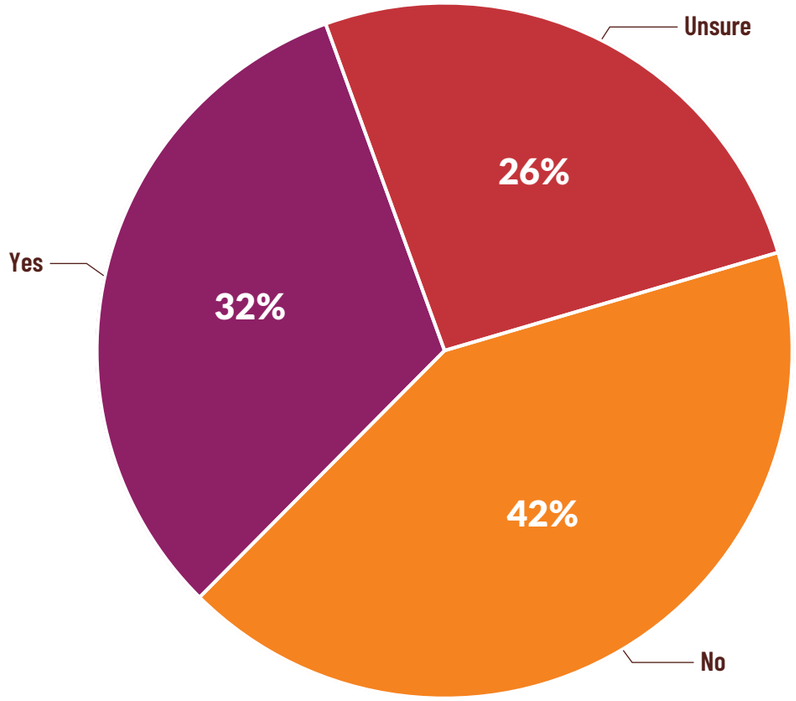
Those working in smaller organizations may have a greater opportunity to work on innovation activities: 60% of respondents in organizations with fewer than 100 employees reported confidence that their senior leaders understood how their role can enable growth and innovation; only 27% of those who work in organizations with 5,000 to 25,000 employees reported the same sureness.

Looking at industry type, those organizations in the technology/telecommunications, business services and legal sectors reported this confidence in their senior leaders at higher rates compared to other industry sectors — 49%, 62% and 50%, respectively.

One reason for these differences could potentially be related to the leadership structures present in each industry sector. Those whose senior leadership is more embedded within the organization's digital governance approach — something more probable in the technology/telecommunications sector, for example — have a better understanding of the key issues, challenges and benefits of a particular approach. As a result, they are more likely to understand how they can enable downstream innovation.

Understanding and appreciation of innovation and growth may also empower and inspire confidence in compliance. A greater proportion of respondents report more confidence in compliance when there is belief from senior leadership that digital governance is a driver of innovation. One likely reason for this is that when governance functions are viewed as enabling growth then those functions are potentially more likely to secure the necessary investment and attention from senior leaders to both manage risks and enable progress.

Confidence that senior leaders understand how your role can enable growth and innovation, overall



Respondents who were confident in their senior leaders' understanding of their role were far more likely to identify that their governance strategies were aligned compared to those who were less confident. Alignment between organizational strategy and governance strategy is crucial for organizational success.

There is broad recognition that governance strategies should support, not hinder, the wider strategy of the organization. Digital governance professionals may be better able to anticipate upcoming projects and strategic shifts, meaning they can plan and support accordingly. Alignment can also help highlight areas in which staff may need additional upskilling due to strategy shifts within the organization.

Finally, greater alignment may support organizational risk strategy approaches, as digital governance professionals will have a better understanding of the risk landscape and thus can provide support and prioritize resources on the most pressing, highest-risk business activities.

Alignment between organizational stategy and governance strategy is crucial for organizational success.

		Are you confident that senior leaders in your organization understand and/or appreciate how your role can be enabling for innovation and growth?	
	Alignment with our organizational strategy	**Yes**	**No**
Privacy	Somewhat or less	14%	45%
	At least to a considerable degree	86%	55%
AI	Somewhat or less	26%	57%
	At least to a considerable degree	74%	43%
Digital responsibility	Somewhat or less	19%	51%
	At least to a considerable degree	81%	49%

Proportion of those reporting compliance challenges that are also confident that senior leaders appreciate innovation and growth capabilities of their role, overall

Identified challenges when delivering on privacy compliance	Confident that senior leaders in the respondent's organization understand and/or appreciate how your role can be enabling for innovation and growth	Not confident that senior leaders in the respondent's organization understand and/or appreciate how your role can be enabling for innovation and growth
Lack of privacy function representation in senior levels of the organization	18%	82%
Privacy team is siloed and is therefore not integrated with other teams	23%	77%
Ineffective integration of privacy risk management within broader risk management activities within the organization	22%	78%
Lack of board support for privacy compliance	11%	89%
No challenges identified	100%	0%

Identified challenges when delivering on AI governance	Confident that senior leaders in the respondent's organization understand and/or appreciate how your role can be enabling for innovation and growth	Not confident that senior leaders the respondent's organization understand and/or appreciate how your role can be enabling for innovation and growth
Lack of structured communication methods across the organization	28%	72%
Lack of AI governance representation in senior levels of the organization	29%	71%
Organizational AI expectations are not clearly defined/followed up on	29%	71%
Ineffective integration of AI risk management within broader risk management activities within the organization	23%	77%
Lack of board support for privacy compliance	0%	100%
No challenges identified	67%	33%

Where respondents identified that senior leaders understood how their governance roles could be enabling for innovation and growth, just over half reported no security incidents and/or data breaches in the last 12 months.

However, where there was no confidence that senior leaders understood innovation capabilities, 70% of those organizations identified there had been some form of breach. While there may be several reasons an organization may experience a security incident and/or data breach, respondents in these organizations that also identified a lack of senior leadership buy-in may seek to increase awareness of the need to address root causes of incidents as well as mature the approach to compliance to adequately consider growth and innovation capabilities.

Those with the capacity to do so should consider advocating for the importance of digital governance functions, specifically as a driver for innovation and growth.



Where there was no confidence that senior leaders understood how governance can support innovation, 70% of those organizations identified there had been some form of breach.

Looking ahead

The digital governance landscape is increasingly complex and intertwined. As digital technologies continue to innovate and both cross and blur the lines between intra-organizational domains, it is digital governance professionals' responsibility to navigate the complex web.

Unfortunately, there is no silver bullet for success. Instead, organizations are tailoring their approach to digital governance in ways that fit their business model and consumer base. This multidisciplinary, multidomain approach reflects the wider point that organizations are adapting to this entropic environment by establishing and supporting strong governance structures, shaped by the contexts and nuances of their organization.

Finally, it is no longer prudent to view governance as a restriction on growth and innovation. It is not just an exercise in risk mitigation and compliance. Despite the uncertain regulatory environment, organizations have made clear that governance structures have a plethora of benefits beyond compliance. Digital governance is an enabler of growth and innovation for any organization, regardless of sector or size. Senior leadership plays a key role in this, needing to recognize the ways in which governance roles can be enabling for growth and innovation.

With all this in mind, it is up to us, as multifaceted digital professionals, to put our heads together and continue down this winding road.

Our research approach

We focus on delivering accurate, meaningful and actionable research to our members.

The IAPP Research and Insights team focuses on bringing our membership accurate, meaningful and actionable research and insights in a digestible way. We do this by leveraging our team of internal experts and global network of subject matter experts, professionals and volunteer contributors.

Visit the IAPP Resource Center for more resources, including legislation trackers, tools, guidance, surveys and in-depth reports.

Contacts

Connect with the team

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

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

Brandon Lalonde
Research and Insights Analyst, IAPP
blalonde@iapp.org

Follow the IAPP on social media

Published November 2025.

IAPP disclaims all warranties, expressed or implied, with respect to the contents of this document, including any warranties of accuracy, merchantability, or fitness for a particular purpose. Nothing herein should be construed as legal advice.

© 2025 IAPP. All rights reserved.