

2026 Data Security and Compliance Risk

Data Sovereignty Report

Awareness is high. Incidents are higher. How organizations across Canada, the Middle East, and Europe are navigating the new rules of data residency.

Contents

03	Executive Summary	16	Key Findings: Aggregate and Per-Region Trends	34	Implications and Recommendations
07	The Regulatory Landscape: Three Regions, Three Realities	16	Understanding and Awareness	34	Business and Strategic Implications
07	From Jurisdiction to Operations	17	Incidents and Risks	36	Policy and Operational Recommendations
08	Why These Trends Matter	19	Benefits and Opportunities	37	Sovereignty Readiness Checklist
10	Survey Overview and Report Structure	20	Resources and Costs	39	Conclusion
12	Methodology	21	AI Governance	43	Legal Disclaimer About Centiment
12	Survey Design and Data Collection	22	Operational Challenges and Future Planning	44	References
13	Sample Composition and Regional Balance	24	Cross-Analyses: Variations by Key Factors		
14	Analytical Approach	24	Industry Variations		
15	Limitations and Considerations	25	Role and Persona Variations		
		28	Size Variations		
		29	Regional Intersections		
		31	Deeper Cross-Analyses: Compliance, Jurisdictional Reach, and AI Governance		

Executive Summary

Data sovereignty has become a strategic priority for organizations operating across borders. The rules governing where data lives, who can access it, and under what legal authority are shifting rapidly in Canada, the Middle East, and Europe. This report draws on a purpose-built survey of 286 professionals across those three regions to map out how organizations understand, experience, and plan for sovereignty requirements today.

The respondent pool reflects a technology-forward, mid-to-large-enterprise audience. The most common role is IT Manager or Specialist (42%), with CIOs and CTOs making up another 23%. In terms of scale, the largest share of respondents (38%) come from organizations employing between 1,000 and 4,999 people.

From Compliance to Autonomy: Europe's "Plan B" Mindset

Europe's sovereign-cloud demand is shifting from compliance to autonomy. IDC reports that protection against extra-territorial data requests has become the top market driver for sovereign cloud in Europe, reflecting anxiety about foreign access and cross-border legal exposure. Importantly, Europe is not planning a wholesale break from hyperscalers: IDC notes that only 4% of European organizations plan to stop using global public cloud vendors and rely solely on local providers. The emerging model is "glocal" that combines global innovation with local control by using both global and local providers with verifiable safeguards.¹

Self-reported understanding of sovereignty requirements is high and remarkably consistent across regions. Approximately 44% of respondents in each region describe themselves as "very well informed," with no statistically meaningful gap between Canada (44%), the Middle East (45%), and Europe (44%). Yet incident rates vary widely, suggesting that awareness alone is not the differentiator. Implementation maturity and exposure matter more.

Data Sovereignty Understanding by Region

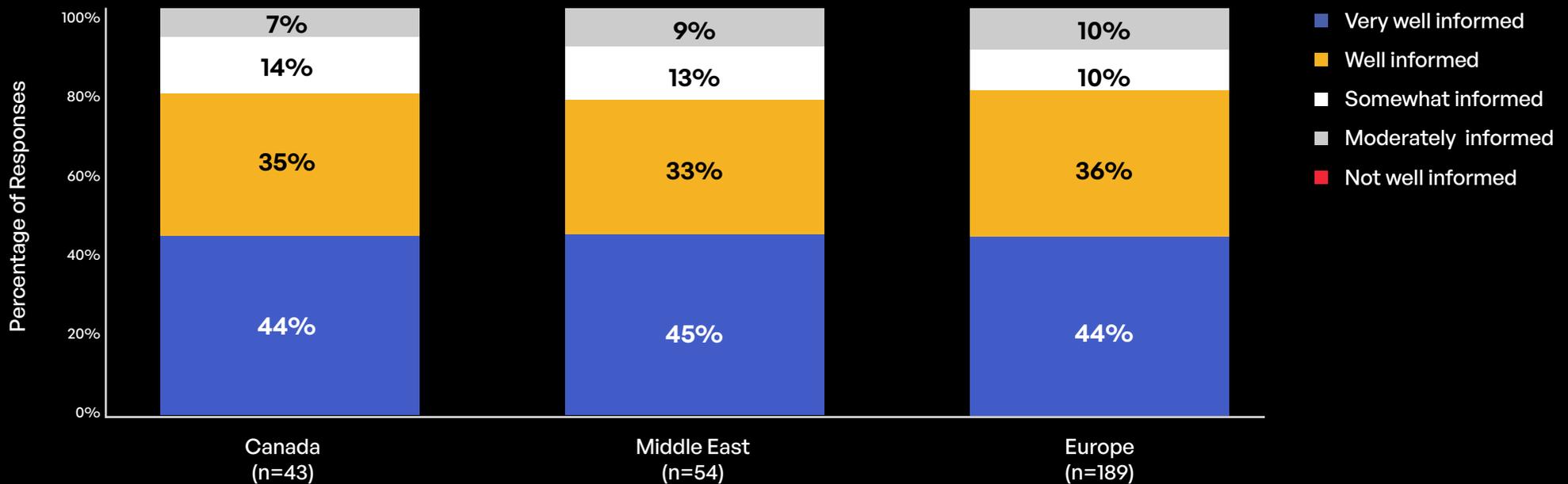


Figure 1: Data sovereignty understanding levels by region (based on 286 survey responses)

One in three respondents (33%) reported experiencing at least one data sovereignty-related incident in the past 12 months. The Middle East reported the highest rate at 44%, compared to 32% in Europe and 23% in Canada. The most common incident types were data breaches with sovereignty implications (17%) and third-party compliance failures (17%), followed by regulatory investigations (15%) and unauthorized cross-border transfers (12%).

Data Sovereignty Incidents Reported in Past 12 Months

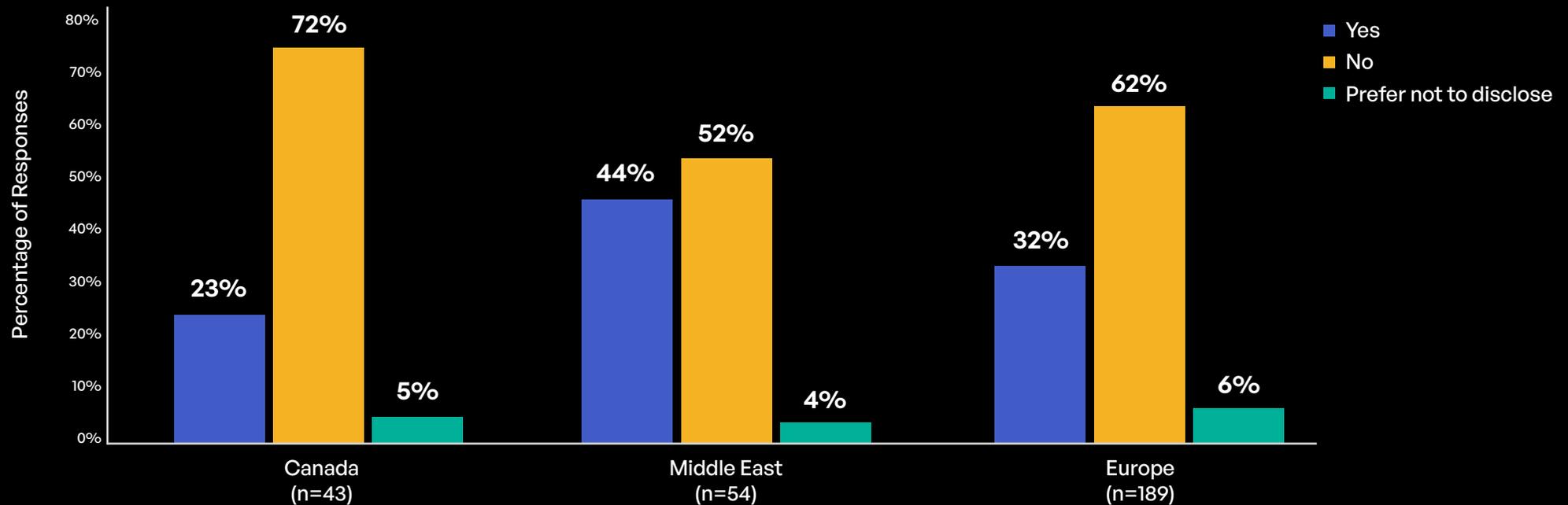
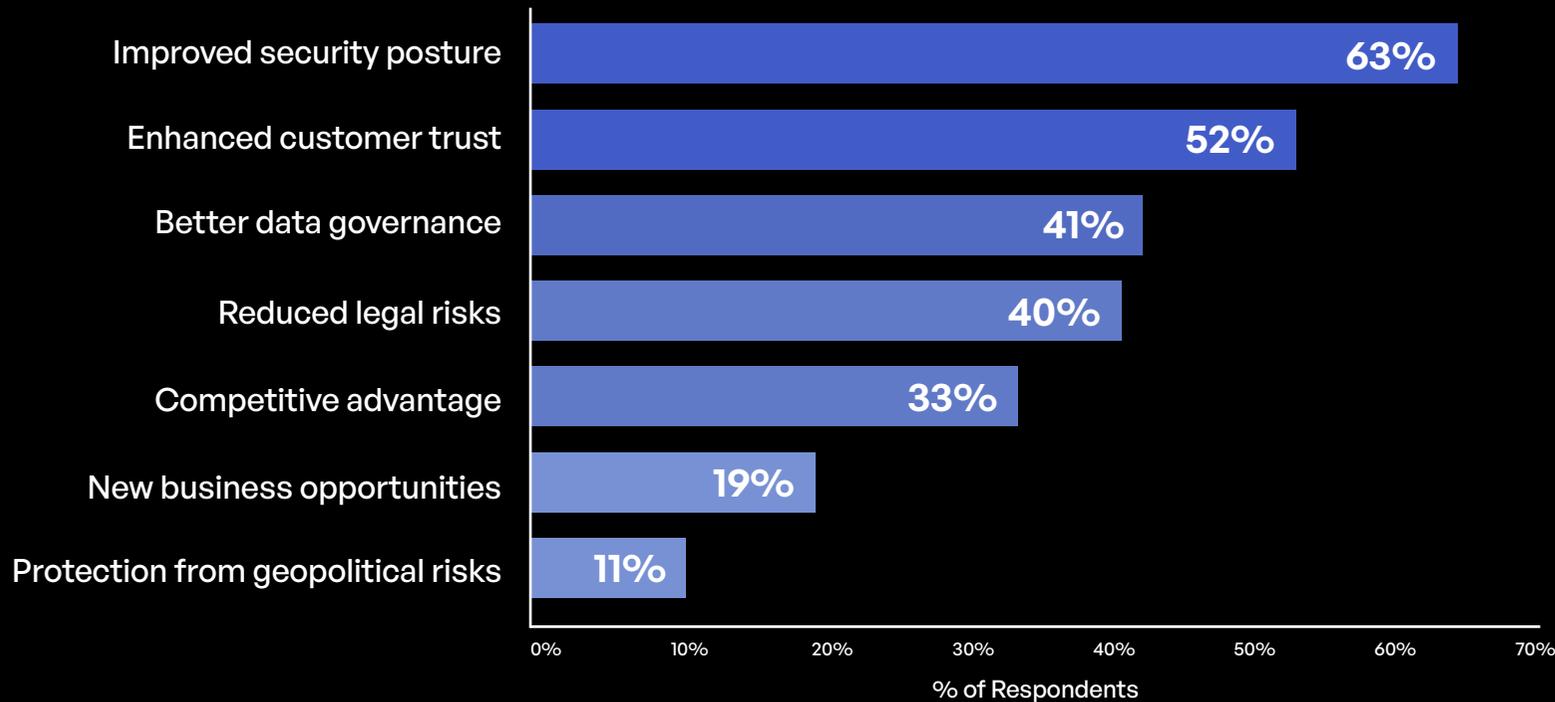


Figure 2: Sovereignty-related incidents reported in the past 12 months, by region

Despite the risks, respondents associate sovereignty compliance with meaningful business benefits. Improved security posture tops the list at 63%, followed by enhanced customer trust (52%), better data governance (41%), and reduced legal risks (40%). Technical infrastructure changes (59%) and legal expertise (53%) rank as the two most resource-intensive areas. Among organizations with 20,000 or more employees, approximately 45% report spending in the top local-currency tier (more than 5 million in CAD, USD, or EUR).

Primary Business Benefits of Data Sovereignty Compliance



For organizations managing AI, a mixed management approach based on data sensitivity is the most common strategy (34%), with regular AI audits (50%) and impact assessments (48%) serving as the primary safeguards. Looking ahead, compliance automation (53%) and enhanced technical controls (50%) lead the two-year planning outlook across all regions. The sections that follow break down these trends in detail.

Figure 3: Primary business benefits experienced from data sovereignty compliance (aggregate)

The Regulatory Landscape: Three Regions, Three Realities

From Jurisdiction to Operations

At its core, data sovereignty is about jurisdiction. It is the principle that data is subject to the laws and governance structures of the country or region where it is collected or stored. In practice, that translates into a growing web of requirements around localization, cross-border transfer restrictions, and the ability to prevent foreign governments or entities from accessing locally held information.

In Europe, the General Data Protection Regulation (GDPA) has been enforceable since 2018, and its impact has been enormous. Combined with the upcoming Data Act (enforcement began in September 2025) and the EU AI Act (GPAI obligations took effect in August 2025), European organizations now operate under one of the most layered sovereignty regimes in the world. Among European respondents in this survey, approximately 15% describe themselves as "extremely concerned" about GDPR fine exposure, reflecting the weight of a cumulative fine tally that has already surpassed €5.66 billion (\$6.74 billion USD).

In Canada, the Personal Information Protection and Electronic Documents Act (PIPEDA) has been the primary framework, with approximately 79% of Canadian respondents reporting full compliance. But the regulatory picture is shifting. Concerns about changes to Canada-U.S. data sharing arrangements rank as the top worry for 40% of Canadian respondents, and 21% flag the U.S. CLOUD Act as a direct threat to their sovereignty posture. These reflect genuine uncertainty about whether data held by U.S.-owned cloud providers can truly remain under Canadian jurisdiction.

Canada Is Shifting Toward Deterrence

Canada's enforcement posture is tightening, with provincial regimes providing near-term signals. Ontario's privacy regulator issued the first administrative monetary penalties under the Personal Health Information Protection Act (PHIPA), ordering a CAD\$5,000 penalty against a physician and CAD\$7,500 against a clinic. Quebec's Law 25 adds higher ceilings, including administrative monetary penalties up to C\$10M or 2% of worldwide turnover, and penal fines up to C\$25M (\$18.43M USD) or 4%. Federal reform proposals have also pointed toward high-ceiling penalties nationally, which would further elevate data-flow control and auditability as core sovereignty requirements.²

The Middle East represents the fastest-moving regulatory environment of the three. Saudi Arabia's Personal Data Protection Law (PDPL) and the Saudi Data and Artificial Intelligence Authority (SDAIA) framework have created a new set of obligations that 93% of Middle Eastern respondents say directly impact their operations. Geopolitical instability in the region (cited by 33% as a top concern) adds a layer of unpredictability that doesn't exist in the same way in Canada or Europe. Regulatory uncertainty around these newer frameworks remains high, with 37% of Middle Eastern respondents identifying it as a key barrier to adopting regional cloud providers.

Sovereignty Isn't Just “Where the Data Sits”

Data sovereignty is increasingly judged on control and legal jurisdiction, not only where data is stored. In late 2025, a Canadian court ordered OVHcloud to produce customer data hosted on servers in France, highlighting how cross-border legal demands can collide with sovereign-cloud expectations. The practical takeaway is that local hosting, by itself, may not prevent compelled disclosure. Mature sovereignty programs pair data residency controls with auditable access controls, clear response processes for government requests, and contracts that define how the provider handles extra-territorial demands.³

Why These Trends Matter

The business case for paying attention to data sovereignty goes well beyond avoiding fines. One in three organizations in this survey (33%) reported a sovereignty-related incident in the past year. **The most common types were data breaches with sovereignty implications and third-party compliance failures, each at 17%. These are operational disruptions with real costs, and they are happening at scale.**

At the same time, respondents who take sovereignty seriously report tangible returns. Nearly two-thirds (63%) associate their compliance efforts with improved security posture, and more than half (52%) point to enhanced customer trust. These are perception-based findings from a self-report survey, but the consistency across regions and industries lends them weight.

On the concern front, nearly half of all CIOs and CTOs (49%) fall into the "very" or "extremely" concerned category about regulatory fines. Only about 10% of respondents overall selected "not concerned at all," indicating that fines remain a meaningful leadership concern across all roles and regions.

Enforcement Risk Is Now Board Level

Enforcement pressure is large enough to change board priorities. CMS's GDPR Enforcement Tracker records 2,245 fines totaling about €5.65B (\$6.73B USD), with an average fine of roughly €2.36M (\$2.81M USD, approximate) and a top fine of €1.2B. In parallel, the EU AI Act introduces administrative fines that can reach €35M (\$41.7M USD) or 7% of worldwide annual turnover for certain violations. For sovereignty and AI governance, proof of control is becoming as important as prevention, because regulators can penalize weak governance, not just breaches.⁴

Concern About Regulatory Fines by Professional Role

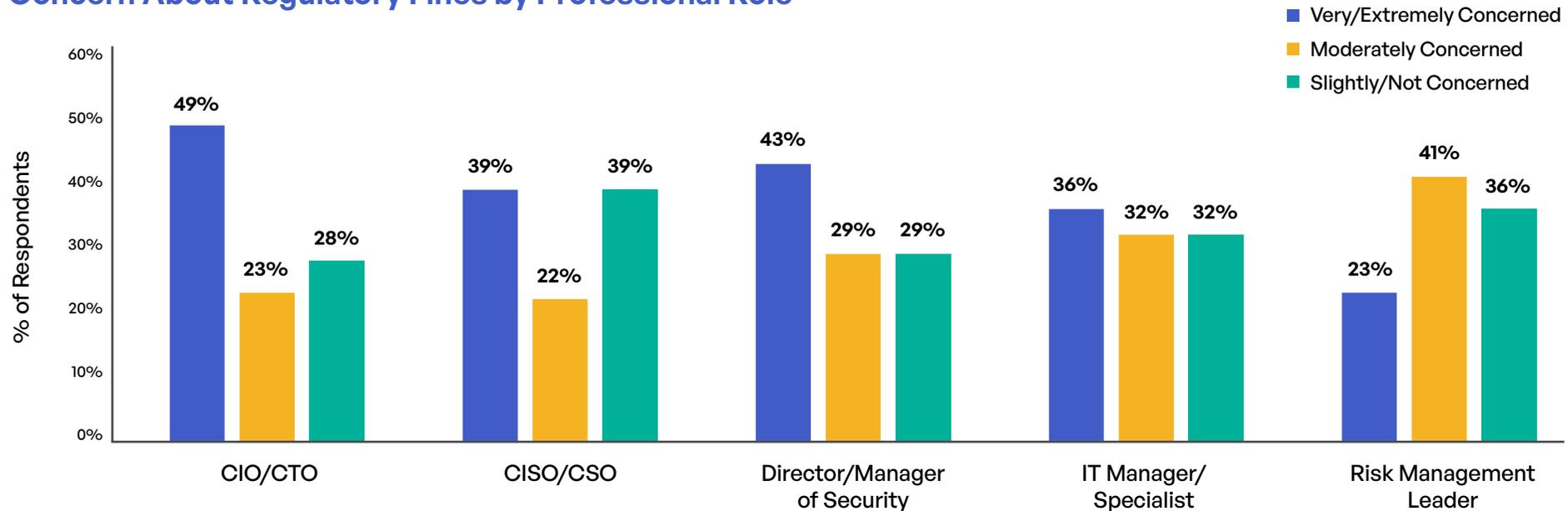


Figure 4: Concern about regulatory fines by professional role

Survey Overview and Report Structure

This report is built on a survey of 286 professionals working in data governance, IT security, risk management, and compliance across Canada (43 responses), the Middle East (54 responses), and Europe (189 responses). The survey covered seven major topic areas: demographics, sovereignty understanding, incidents, business benefits and resource requirements, AI data governance, future planning, and regulatory concerns.

When it comes to organization size, the largest cluster sits in the 1,000 to 4,999 employee range (38%). Larger enterprises with 10,000 or more employees make up about 22% of the sample.

Respondent Distribution by Professional Role

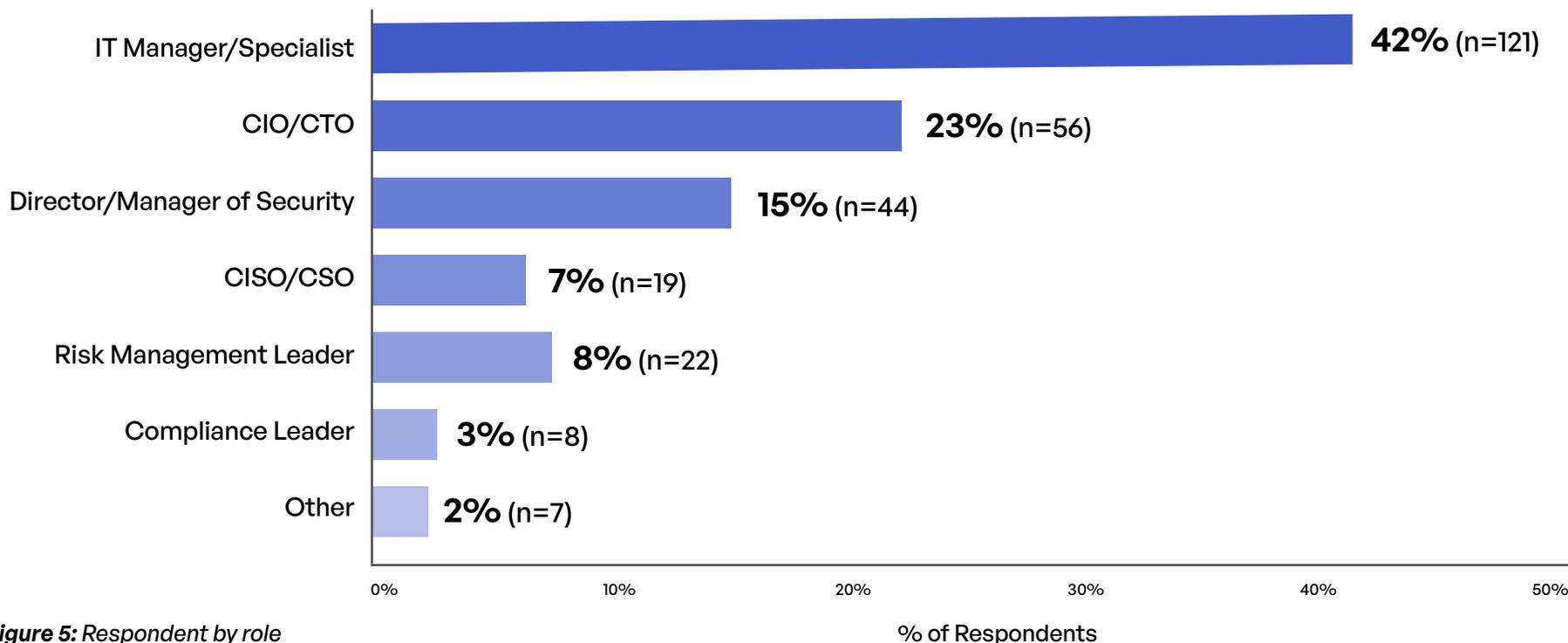


Figure 5: Respondent by role

Respondent Distribution by Organization Size

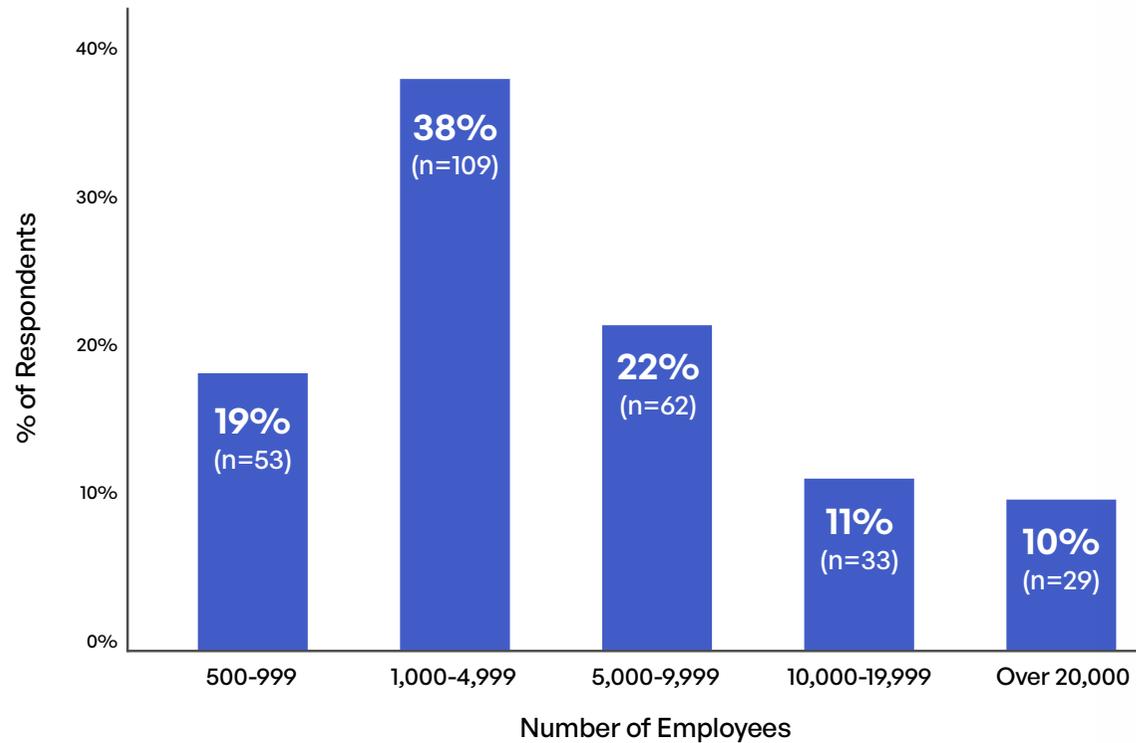


Figure 6: Respondent distribution by organization size

The report is organized into five core sections following this introduction. Methodology explains data collection and analysis. Key Findings presents aggregate and per-region results. Cross-Analyses examines variations by industry, role, and organization size. The Implications and Recommendations section synthesizes the data into guidance. And the Conclusion ties it together with a forward-looking view.

Methodology

Survey Design and Data Collection

The data behind this report comes from a structured online survey administered across three separate regional cohorts: Canada, the Middle East, and Europe. Each regional version was tailored to reference the specific regulations, cloud providers, and geopolitical factors relevant to that geography, while maintaining a shared core of questions to allow direct comparison. The survey covered seven major topic areas: demographics, sovereignty understanding, incidents, business benefits and resource requirements, AI data governance, future planning, and regulatory concerns.

Question formats varied by topic. Demographic questions used single-select categorical fields. Sovereignty understanding was captured on an ordinal scale ranging from "Not well informed" to "Very well informed." Incident questions used a binary yes/no gate followed by a multi-select list of incident types. Benefits, resources, and planning questions allowed respondents to select up to three options from a predefined list, which means percentages for those items can exceed 100% when summed. AI governance included both a single-select management question and a multi-select list of safeguards. Communication channel challenges were rated on a matrix scale, and implementation challenges were ranked on a 1-to-6 scale where 1 represented the most challenging.

Table 1: Survey Details, Methodology, and Approach

Element	What We Did	How It Shows Up in This Report
Study format	Structured online survey across three regional cohorts (Canada, Middle East, Europe) with a shared core questionnaire	Enables direct cross-region comparison on core measures plus region-specific context where needed
Respondent base	286 total responses across the three regions	All charts and cross-analyses reference this base unless otherwise noted
Topic modules covered	Seven modules: demographics, sovereignty understanding, incidents, benefits and resource needs, AI data governance, future planning, regulatory concerns	Mirrors the report's section flow (awareness → incidents → benefits/costs → AI governance → planning)
Question types used	Single-select, multi-select (up to 3), matrix ratings, and ranked-choice items	Multi-select totals can exceed 100%; ranked items are summarized using mean rank
Incident measurement	Yes/No incident "gate" + follow-on incident-type selections	Report shows both overall incident rate and the most common incident categories
Reporting convention	Percentages are presented on a comparable basis across regions	Regional comparisons are displayed as within-region distributions (to avoid distortion from uneven sample sizes)
Analysis approach	Aggregation + crosstabs by region/industry/role/org size	Figures show "by region/industry/role/size" breakdowns consistently across topics
Validation	Results were verified through computational checks	Provides confidence that charts and crosstabs reflect the underlying survey outputs

Sample Composition and Regional Balance

The survey collected 286 complete responses: 43 from Canada (15%), 54 from the Middle East (19%), and 189 from Europe (66%). **All percentages reported in this study are calculated within each region (row-normalized), so the uneven sample sizes do not distort regional comparisons.**

The regional samples differ in meaningful ways beyond size. Europe is more heavily weighted toward Technology and Software (60%) and Financial Services (23%), while Canada has the strongest Manufacturing representation (21%). The Middle East stands out for its concentration of larger organizations, with 30% of respondents working at companies with 10,000 to 19,999 employees. These compositional differences are accounted for through normalized crosstabs rather than raw counts.

Response Distribution by Region: Industry, Role, and Organization Size

	Industry (%)					Role (%)				Organization Size (%)				
Canada	49%	12%	21%	7%	2%	33%	20%	23%	5%	23%	30%	26%	7%	14%
Middle East	53%	13%	15%	4%	6%	43%	19%	17%	11%	9%	33%	19%	30%	9%
Europe	60%	23%	7%	3%	2%	47%	26%	14%	6%	20%	41%	22%	7%	10%
	Tech/ Software	Financial Services	Mfg.	Gov/ Public	Healthcare	IT Mgr./ Spec.	CIO/ CTO	Dir./Mgr. Security	CISO/ CSO	500- 999	1,000- 5,000	5,000- 10,000	10,000- 20,000	Over 20,000

Figure 7: Response distribution by region across industry, role, and organization size (row-normalized percentages)

Analytical Approach

Analysis was conducted in Python using Pandas for data manipulation and computation. The process followed a five-stage pipeline, moving from raw data collection through to verified findings. The first step was loading and inspecting the three regional datasets independently. The second step unified the data, identifying 86 columns that were common or semantically equivalent across all three surveys. Aggregate analysis produced value counts and percentages for categorical questions, selection rates for multi-select items, and mean rank scores for ranking questions. Cross-tabulation used row-normalized percentages to compare distributions across regions, industries, roles, and organization sizes.

Analysis Pipeline: From Raw Survey Data to Verified Findings

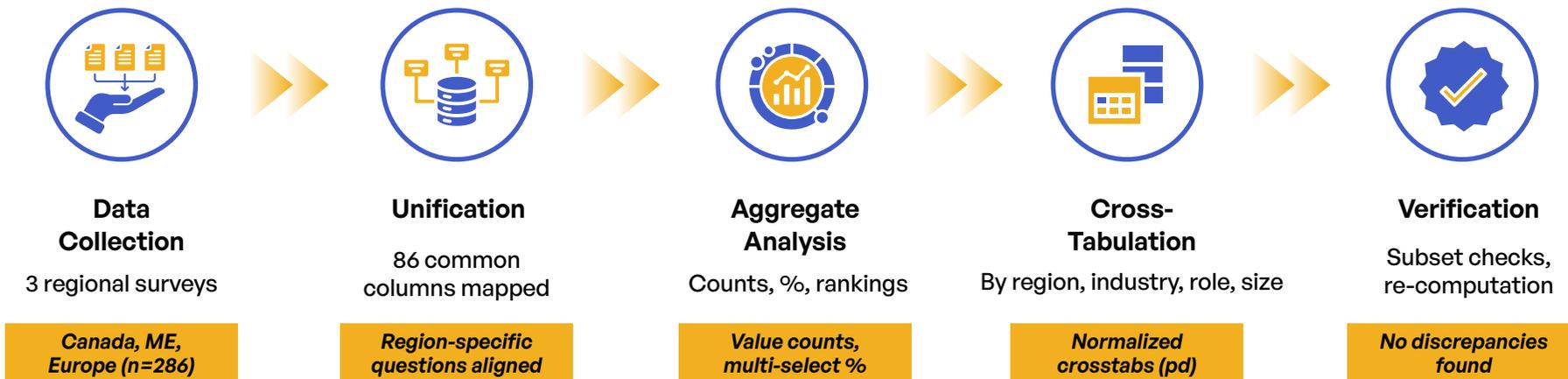


Figure 8: Five-stage analysis pipeline from raw survey data to verified findings

Every computed result went through a verification step. Subset checks compared statistics derived from partial records against full-dataset results. For selected questions, crosstabs were independently re-computed using an alternative method to confirm identical outputs. No discrepancies were found at any verification stage.

Limitations and Considerations

Several limitations are worth flagging. First, this is a self-report survey. Respondents may over-report their understanding or under-report incidents, particularly in regions where enforcement carries reputational risk. The 6% of European respondents who selected "prefer not to disclose" on the incidents question hints at this dynamic.

Second, the regional surveys used different currencies for compliance spending questions (euros for Europe, U.S. dollars for the Middle East, and Canadian dollars for Canada), which limits the ability to make precise cross-regional spending comparisons. Where spending is discussed, local-currency tiers are referenced rather than converted figures.

Third, region-specific questions (such as those referencing the CLOUD Act for Canada or the AI Act for Europe) cannot be compared directly across regions. These are reported within their respective regional contexts and used to enrich the narrative rather than as a basis for cross-regional statistical claims.

Key Findings: Aggregate and Per-Region Trends

This section walks through the core findings of the survey, moving topic by topic through sovereignty understanding, incidents, benefits, resources, AI governance, and future planning. For each topic, the aggregate picture is presented first, followed by the regional and demographic breakdowns that reveal where organizations diverge.

Understanding and Awareness

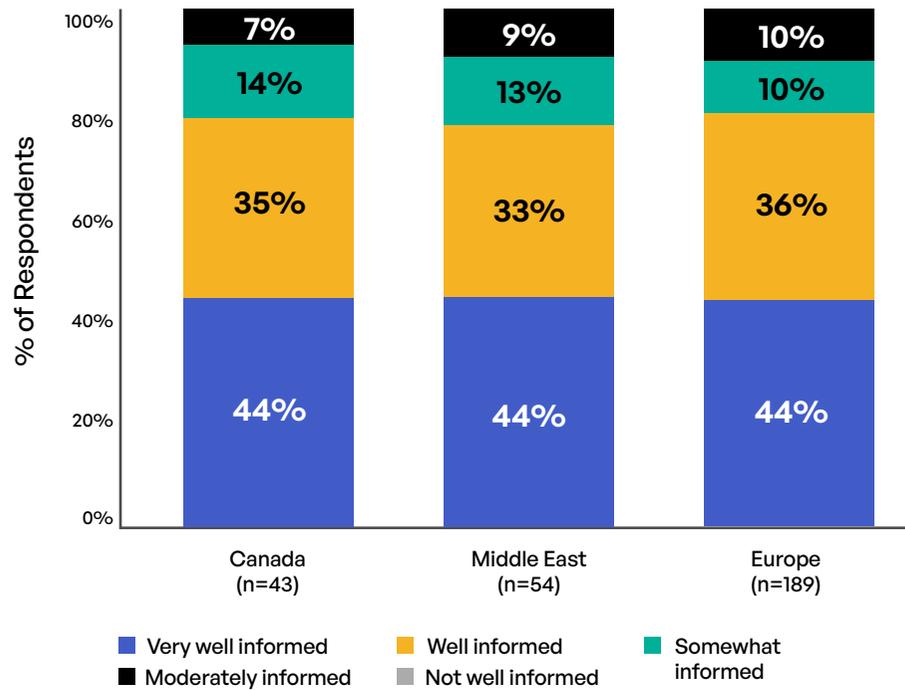
Across the full sample, approximately 44% of respondents describe themselves as "very well informed" about data sovereignty requirements, and another 36% say they are "well informed." **That means roughly four in five respondents (80%) feel they have a solid working knowledge of the rules governing their data.** About 10% fall into the "somewhat informed" category, and roughly 9% land on "moderately" or "not well informed."

The most striking finding on understanding is what doesn't vary: regional awareness is nearly flat. Canada, the Middle East, and Europe all report approximately 44% in the "very well informed" tier. This challenges the assumption that Europe's longer regulatory history under GDPR has produced meaningfully higher self-reported confidence. What the data suggests instead is that awareness has caught up across regions, even where frameworks like PDPL and SDAIA are newer. The differentiator is not whether people know the rules exist but how effectively their organizations implement them.

Industry shapes awareness more than region does. Technology and Software professionals report the highest confidence at 48% "very well informed," followed by Financial Services at 45%. Manufacturing drops to 41%, and Government and Public Sector comes in at 36%. Role matters even more: A meaningful awareness gap exists between security-focused roles and IT implementation staff, the largest respondent group.

Sovereignty Understanding: Regional and Industry Breakdown

By Region



By Industry

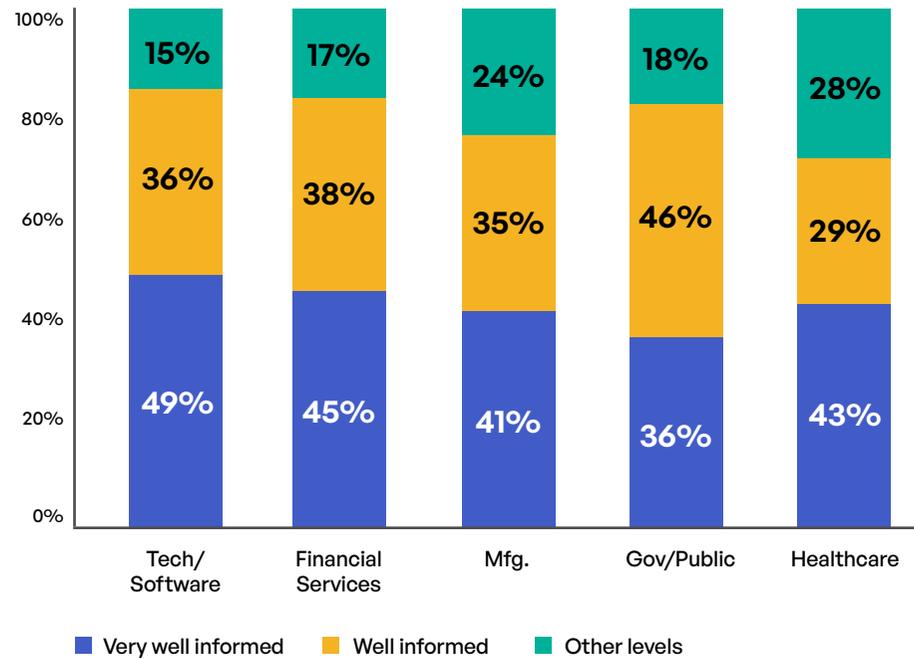


Figure 9: Sovereignty understanding levels by region (left) and by industry (right)

Incidents and Risks

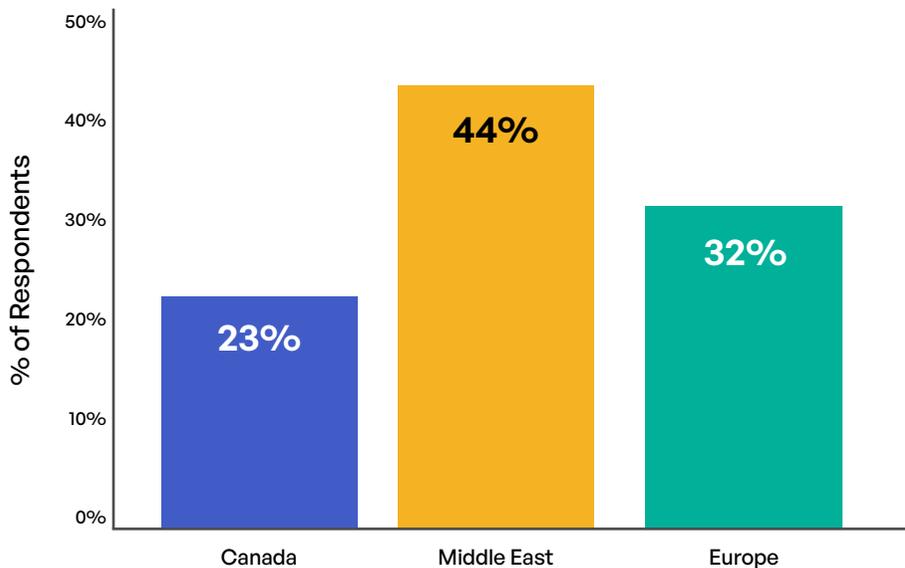
One in three respondents (33%) reported experiencing a data sovereignty-related incident in the past 12 months. **Another 5% preferred not to disclose, which likely means the true figure is higher.** Data breaches with sovereignty implications and third-party compliance failures were each cited by 17% of the full sample. Regulatory investigations or audits hit 15%, unauthorized cross-border transfers 12%, and government data access requests 10%.

The Middle East stands out with the highest incident rate at 44%, nearly double Canada’s 23%. Europe sits at 32%. Several factors likely contribute to the Middle East’s position: the relative newness of its regulatory frameworks creates compliance gaps, larger organizations in that sample present bigger attack surfaces, and the region’s geopolitical volatility adds a dimension of risk that doesn’t exist in the same way elsewhere.

Organization size shows a clear relationship with incident rates. Companies with over 20,000 employees report approximately 45% in the top spending tier, compared to 28% for those with 500 to 999 employees. The trend line varies across size brackets, with larger organizations facing broader compliance footprints and greater exposure to cross-border complexity to regulators, partners, and threat actors.

Sovereignty Incidents in Past 12 Months: By Region and Organization Size

By Region (% "Yes")



By Organization Size (% "Yes")

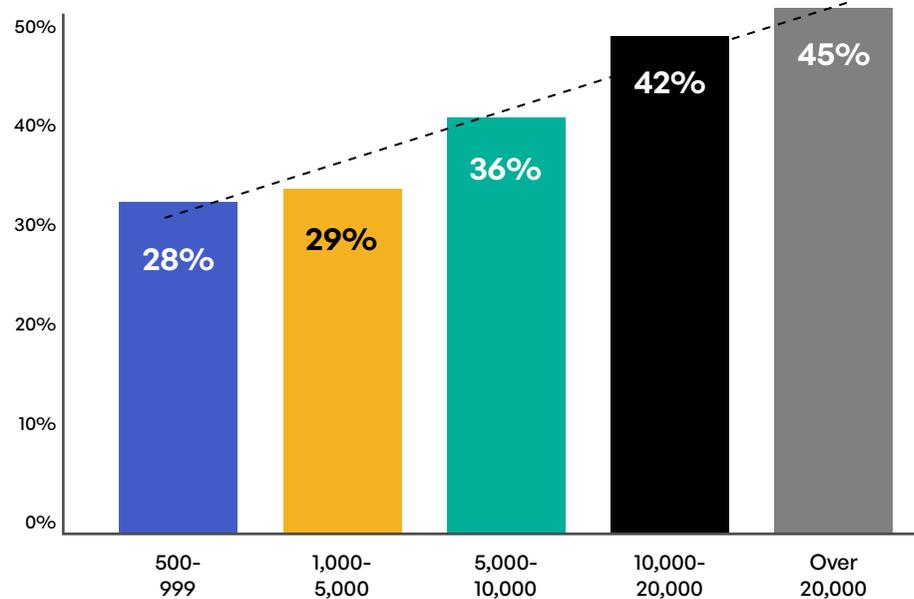


Figure 10: Sovereignty incidents by region (left) and by organization size with trendline (right)

Benefits and Opportunities

When respondents were asked to identify the primary business benefits they associate with sovereignty compliance, the results tell an encouraging story. **Improved security posture leads at 63%, followed by enhanced customer trust at 52%, better data governance at 41%, and reduced legal risks at 40%.** A third (33%) point to competitive advantage, and nearly one in five (19%) report new business opportunities.

Regional differences in benefit perception are relatively narrow. Canada and the Middle East both rate security posture as the top benefit, with Europe close behind. The consistency across regions suggests that sovereignty compliance is broadly associated with stronger security outcomes regardless of regulatory maturity.

Protection from geopolitical risks sits at the bottom of the list at 11% overall, but the Middle East reports the highest rate on that measure, roughly 50% higher than the other two regions. That gap underscores how sovereignty means different things in different contexts.

Business Benefits of Sovereignty Compliance by Region

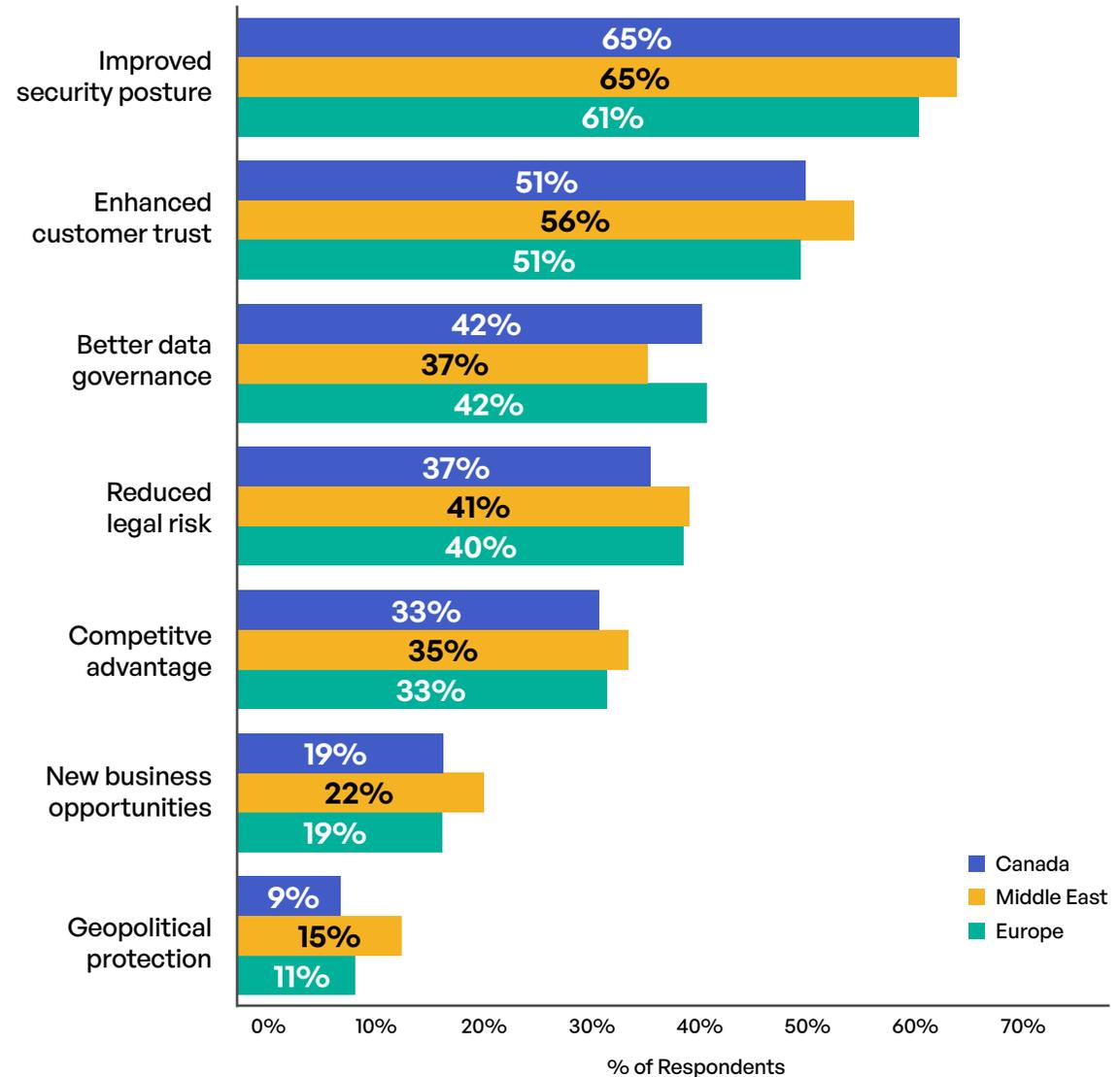


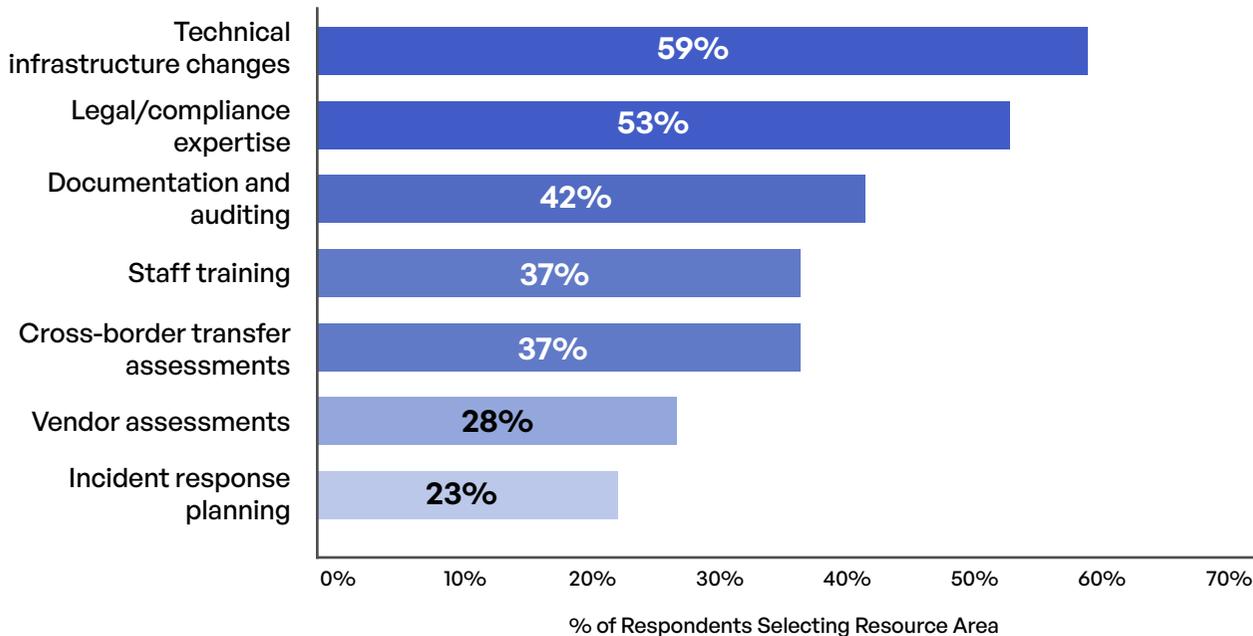
Figure 11: Business benefits of sovereignty compliance, compared across three regions

Resources and Costs

Compliance doesn't come free. **Technical infrastructure changes top the resource list at 59%, followed by legal and compliance expertise at 53%.** Documentation and auditing comes in third at 42%, followed by staff training and cross-border transfer assessments (both at 37%), vendor assessments (28%), and incident response planning (23%).

The technical burden is consistent across all three regions, ranging from 58% in Europe to 65% in Canada. The more interesting variation shows up in secondary priorities: Canada puts relatively more weight on documentation and auditing, the Middle East on cross-border transfer assessments, and Europe on staff training. The relative emphasis on these secondary areas maps to the specific compliance challenges each region faces.

Compliance Resource Requirements



On spending, the picture scales with organization size. Among companies with over 20,000 employees, approximately 45% report spending in the top local-currency tier (more than 5 million in CAD, USD, or EUR). For the 10,000 to 19,999 bracket, that drops to approximately 18%. Mid-sized organizations (1,000 to 4,999) are heavily concentrated in the lower tiers. By industry, Financial Services stands out with a higher share of respondents in elevated spending categories, reflecting tighter regulatory requirements and the complexity of managing sovereignty across global banking operations.

Figure 12: Proportion of compliance resource requirements across seven categories (aggregate)

AI Governance

AI introduces a new dimension to the sovereignty conversation, and most organizations are still figuring it out. The most common approach to managing AI training data is a mixed strategy based on data sensitivity, selected by 34% of respondents. **Another 36% keep all AI training data within their home region.** About 21% are still developing their AI data policy, 5% have no specific location requirements, and 5% report not using AI or machine learning at all.

The safeguard landscape is more developed than the management strategies might suggest. Regular AI audits lead at 50%, followed by impact assessments for high-risk AI at 48%, consent management at 46%, and transparency documentation at 45%. Bias testing and monitoring comes in at 37%, and regulatory sandboxes for AI testing at 36%. Only 4.5% report having no safeguards in place.

Industry differences in safeguard adoption are notable. Financial Services leads on regular audits at 59%, driven by both regulatory pressure and the sensitivity of financial data used in AI models. Government and Public Sector organizations are the most likely to localize AI data (36%), consistent with public sector mandates around data residency.

AI Safeguard Adoption Rates by Industry

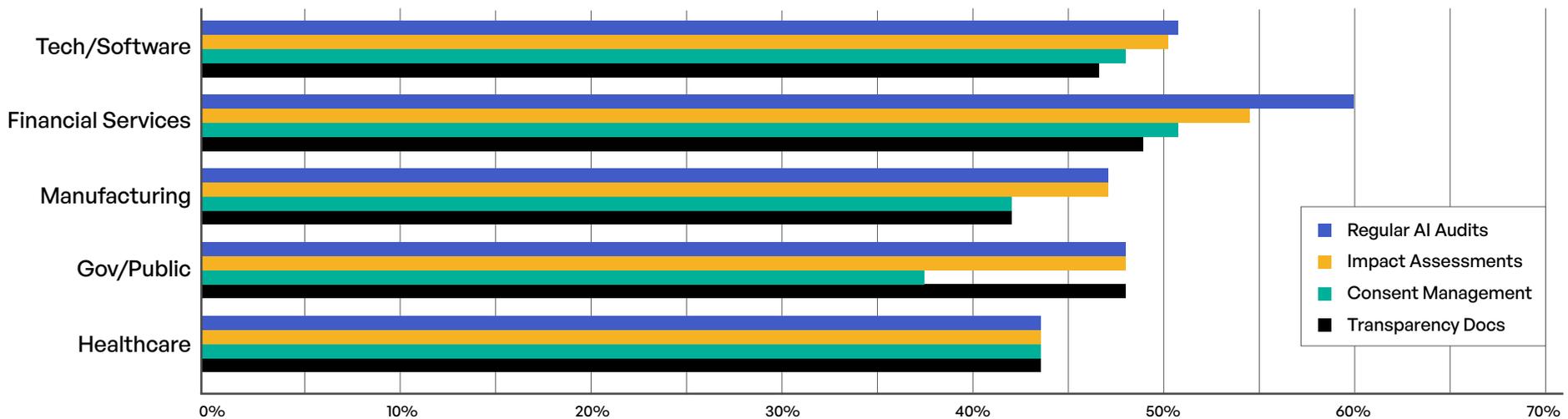


Figure 13: AI safeguard adoption rates across the top five industry sectors

Operational Challenges and Future Planning

When respondents rated the compliance difficulty of different communication channels, email came out as the easiest to manage, with 52% calling it "Easy" and another 32% rating it "Manageable." Cloud file sharing and managed file transfer sit in the middle. SFTP ranks among the trickier channels, with 19% calling it "Challenging" and 6% "Very Challenging." The operational complexity of sovereignty sits primarily in infrastructure redesign, vendor compliance, and cross-border assessments rather than in day-to-day communication tools.

On implementation, respondents ranked technical complexity as the top challenge (mean rank of 3.1 on a 1-to-6 scale), followed by cost of compliance (3.3) and vendor/partner compliance (3.6). Lack of clear guidance and internal resource constraints both ranked lower (3.8).

Looking ahead, the most popular strategy for the next two years is investing in compliance automation, selected by 53% of respondents. **Enhancing technical controls follows at 50%, increasing use of regional cloud providers at 45%, expanding legal and compliance teams at 40%, implementing data localization at 38%, and restructuring international operations at 28%.** Only 4% say they have no significant changes planned.

Regional priorities diverge. Europe leans most heavily toward automation (55%) and expanding legal teams (42%). The Middle East puts the strongest emphasis on regional providers (48%) and restructuring international operations (35%). Canada leads on data localization (42%) but also has the highest rate of "no significant changes planned" (12%), suggesting a split between active investors and those who consider their current posture adequate.

Planned Sovereignty Strategies Over the Next 2 Years, By Region

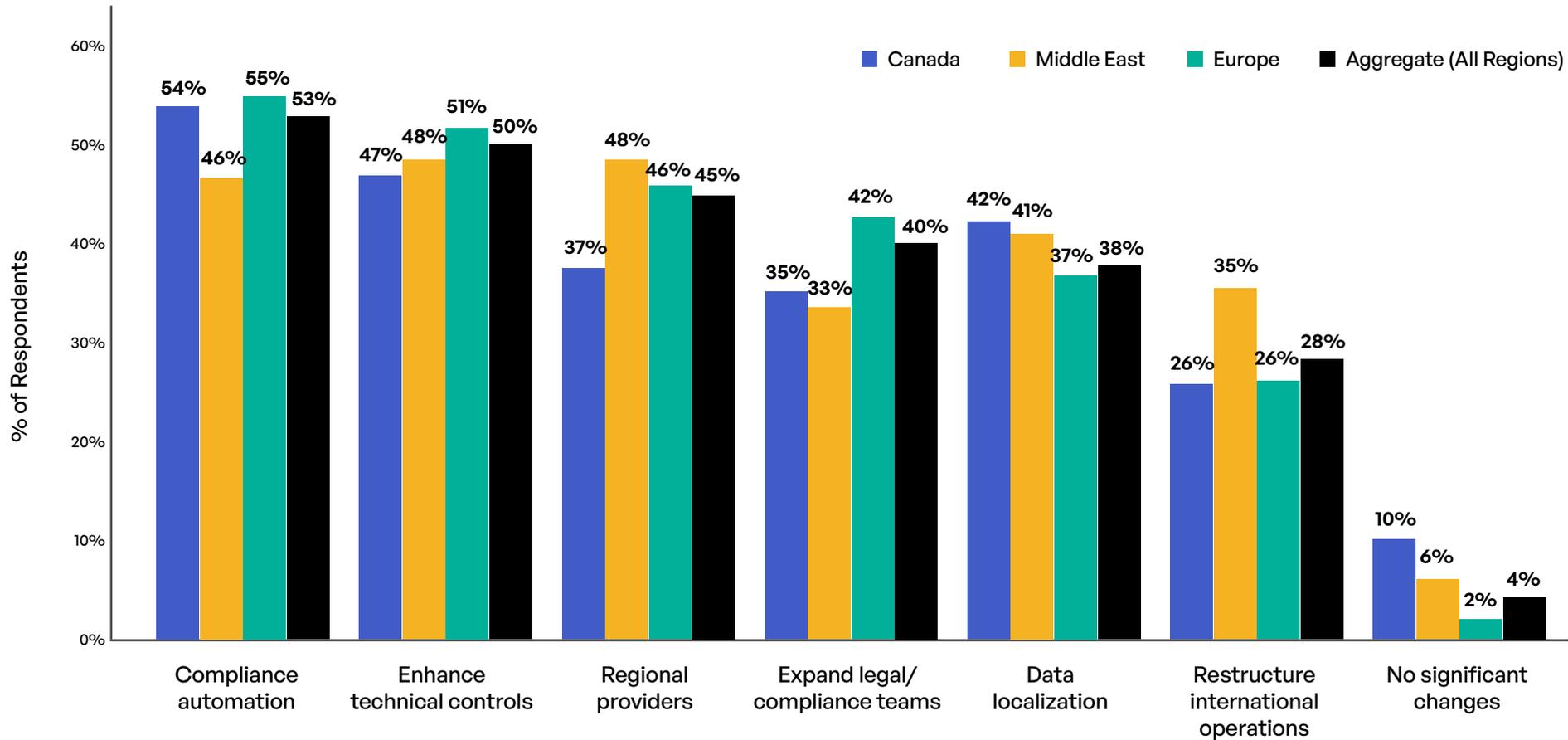


Figure 14: Planned sovereignty strategies over the next two years, by region

Organization size amplifies all these trends. Among companies with over 20,000 employees, 69% plan to invest in compliance automation and 62% in enhanced technical controls. For companies with 500 to 999 employees, those figures drop to 43% each. That imbalance is worth watching as enforcement pressure increases.

Cross-Analyses: Variations by Key Factors

The aggregate findings in the previous section tell one version of the story. This section tells the other. By cutting the data across industry, professional role, organization size, and regional intersections, patterns emerge that the top-line numbers can obscure.

Industry Variations

The two sectors that stand out most sharply are Manufacturing and Financial Services, but for different reasons.

Manufacturing has the highest industry-level incident rate at approximately 52%, the most elevated of any sector.

Manufacturing organizations often face sovereignty challenges through supply chain data flows and cross-border partnerships rather than through direct cloud operations, which may explain why their incident exposure is so high despite moderate awareness levels (41% "very well informed").

Financial Services, meanwhile, is where sovereignty investment runs deepest. It leads on high-tier compliance spending and reports 59% adoption of regular AI audits, well above the aggregate. Technology and Software respondents report the highest sovereignty awareness (48% "very well informed") and the heaviest technical infrastructure burden (63%), which aligns with their cloud-native, cross-border-by-default operating model. Their incident rate sits at approximately 33%, close to the aggregate average.

Government and Public Sector, while a smaller sample (n=11), shows distinctive patterns. It has the lowest "very well informed" rate (36%) and a notable emphasis on AI data localization within its home region. Healthcare follows a similar path on localization but reports the highest email difficulty among all sectors (14% "very challenging"), likely driven by the sensitivity of patient data.

"Very Well Informed" About Sovereignty: Industry and Role Comparison

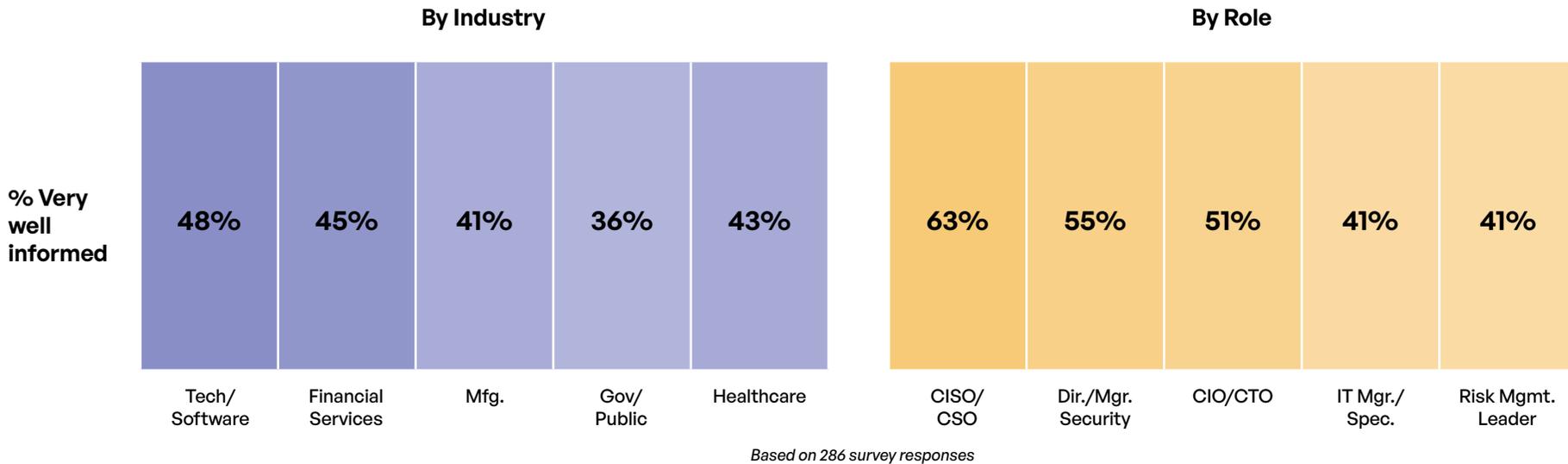


Figure 15: "Very well informed" about sovereignty requirements, by industry and by role

Role and Persona Variations

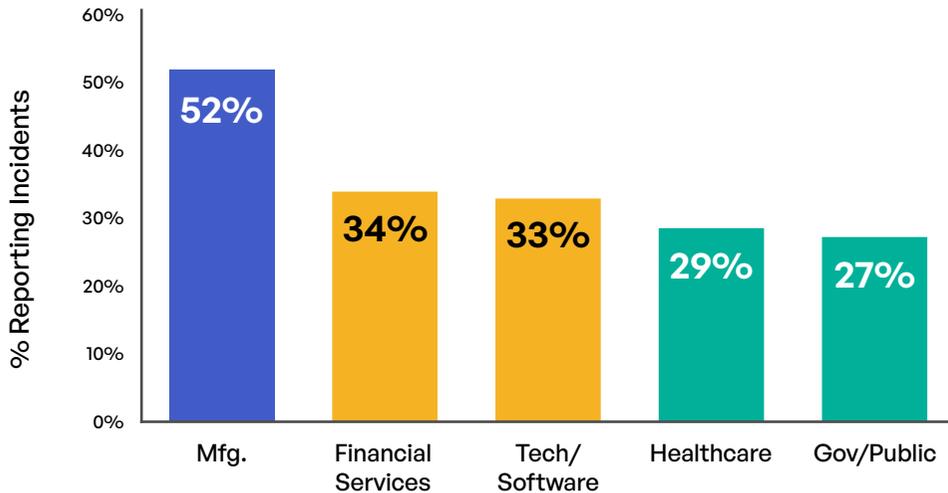
Professional role is one of the strongest predictors of how a respondent experiences data sovereignty. **CISOs and CSOs sit at one end of the spectrum: they report the highest combined demand for legal expertise (68%) and cross-border assessments (58%), and are the roles most likely to have experienced incidents. These are the people closest to the operational reality of sovereignty.**

Security Directors follow a similar but slightly less intense pattern, with strong awareness and notable incident exposure. CIOs and CTOs carry significant awareness levels and moderate incident exposure. They carry the heaviest perceived burden on technical infrastructure (66%), aligning with their role in making infrastructure investment decisions. They also show heightened concern about regulatory fines, consistent with their role in making infrastructure investment decisions.

IT Managers and Specialists, the largest group at 42% of respondents, present the most important workforce finding. **Their awareness lags security-focused roles meaningfully (lagging security-focused roles on key awareness dimensions),** and their incident rate is among the lowest of any role group. That gap may mean they lack the sovereignty awareness needed to prevent issues before they escalate. With 61% citing technical infrastructure as a resource drain, these are the people doing the hands-on implementation work.

Sovereignty Incident Rates: Industry and Role Risk Profiles

Incidents by Industry (% "Yes")



Incidents by Role (% "Yes")

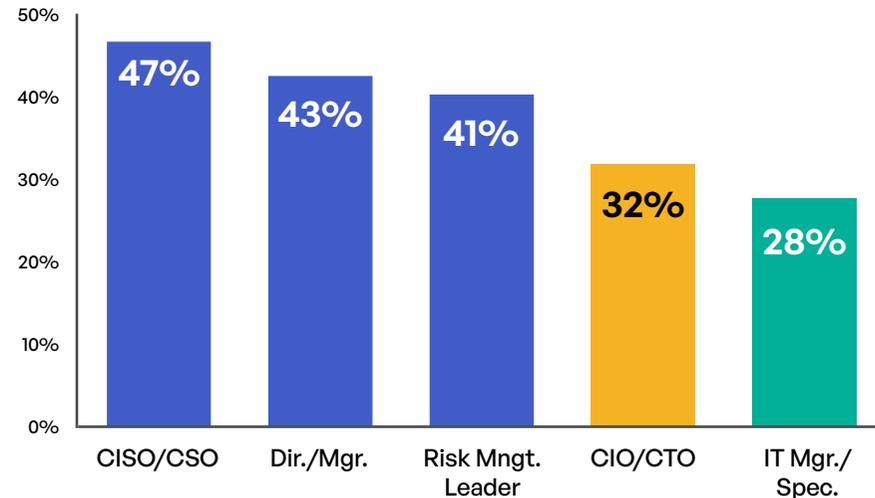


Figure 16: Sovereignty incident rates by industry (left) and by professional role (right)

Risk Management Leaders round out the picture with moderate awareness and a notable incident rate. Their relatively modest numbers on most measures suggest that sovereignty may not yet be fully integrated into enterprise risk frameworks. That could be a gap worth closing.

Compliance Resource Burden by Professional Role

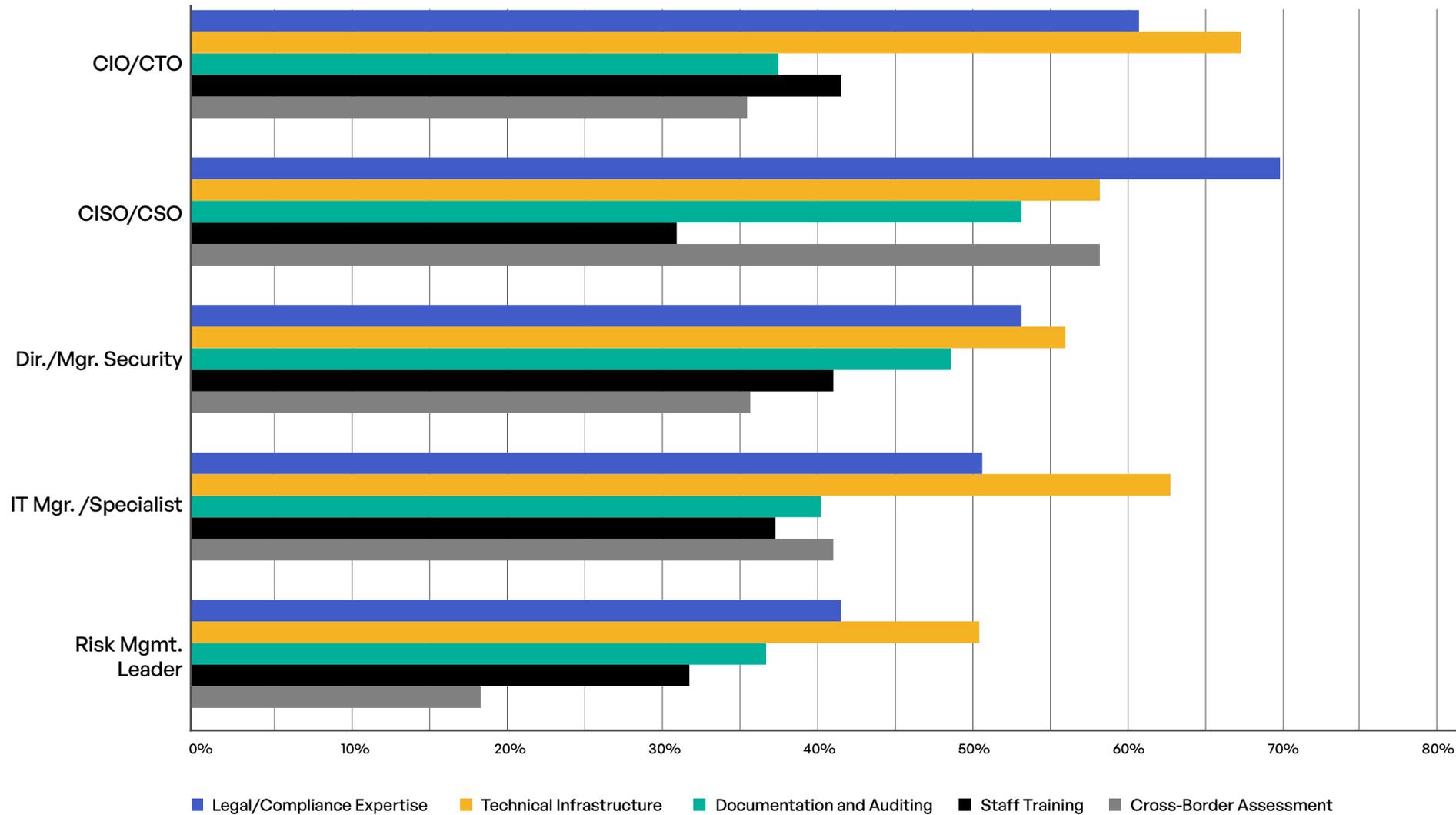


Figure 17: Compliance resource burden across five resource areas, broken down by professional role

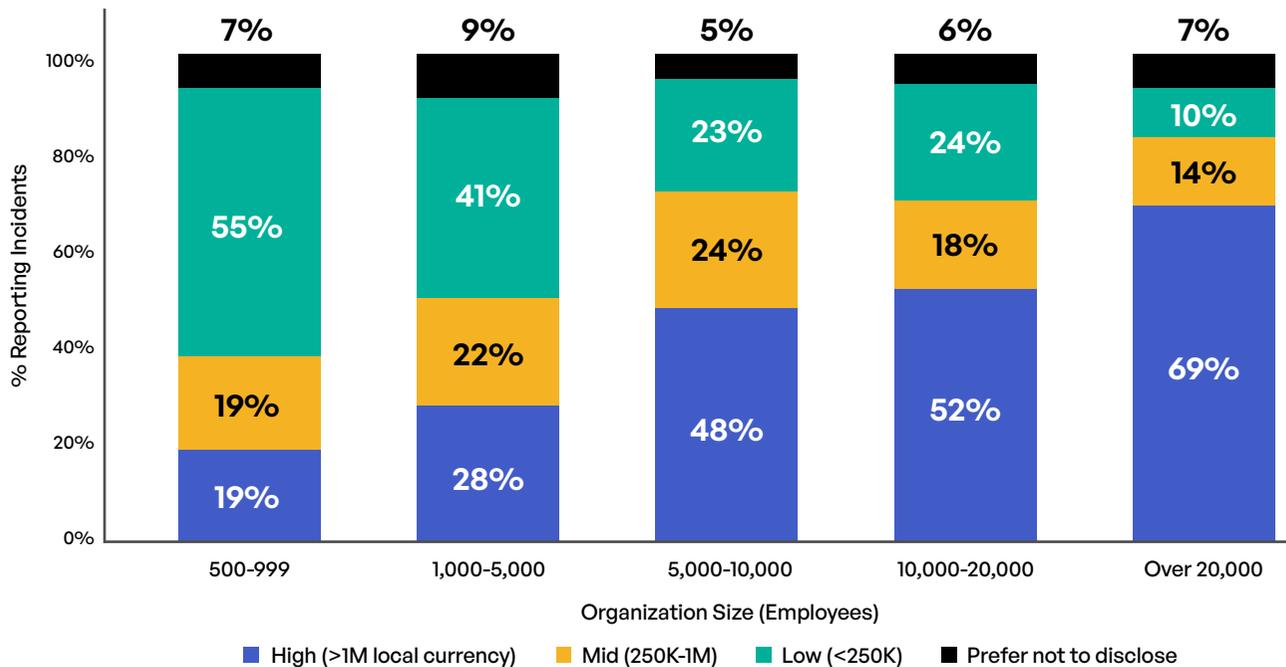


Size Variations

Organization size acts as a multiplier across almost every dimension of sovereignty. **The consistency of this pattern is striking.** Among companies with over 20,000 employees, 55% are "very well informed," 45% have experienced incidents, approximately 45% spend in the top local-currency tier, and 69% plan to invest in compliance automation.

At the other end, organizations with 500 to 999 employees tell a different story. Their awareness sits at 42%, incidents at 28%, and high-tier spending at just 19%. Only 43% plan to invest in automation. The gap between the smallest and largest organizations on nearly every measure is 15 to 25 percentage points.

Annual Sovereignty Compliance Spending by Organization Size



High-tier spending (above 1 million in local currency) rises from 19% among the smallest organizations to 69% among the largest. Mid-tier spending stays relatively flat at 14% to 24%, suggesting a baseline compliance investment that most organizations make regardless of scale. The planning data reinforces the divide: Large organizations lead on every planned strategy except "no significant changes."

Figure 18: Annual sovereignty compliance spending distribution by organization size

Regional Intersections

The final cross-analysis layer looks at how the three regions differ on specific barriers, concerns, and strategic choices that reflect their unique operating environments.

Barriers to Adopting Regional Cloud Provider, by Region

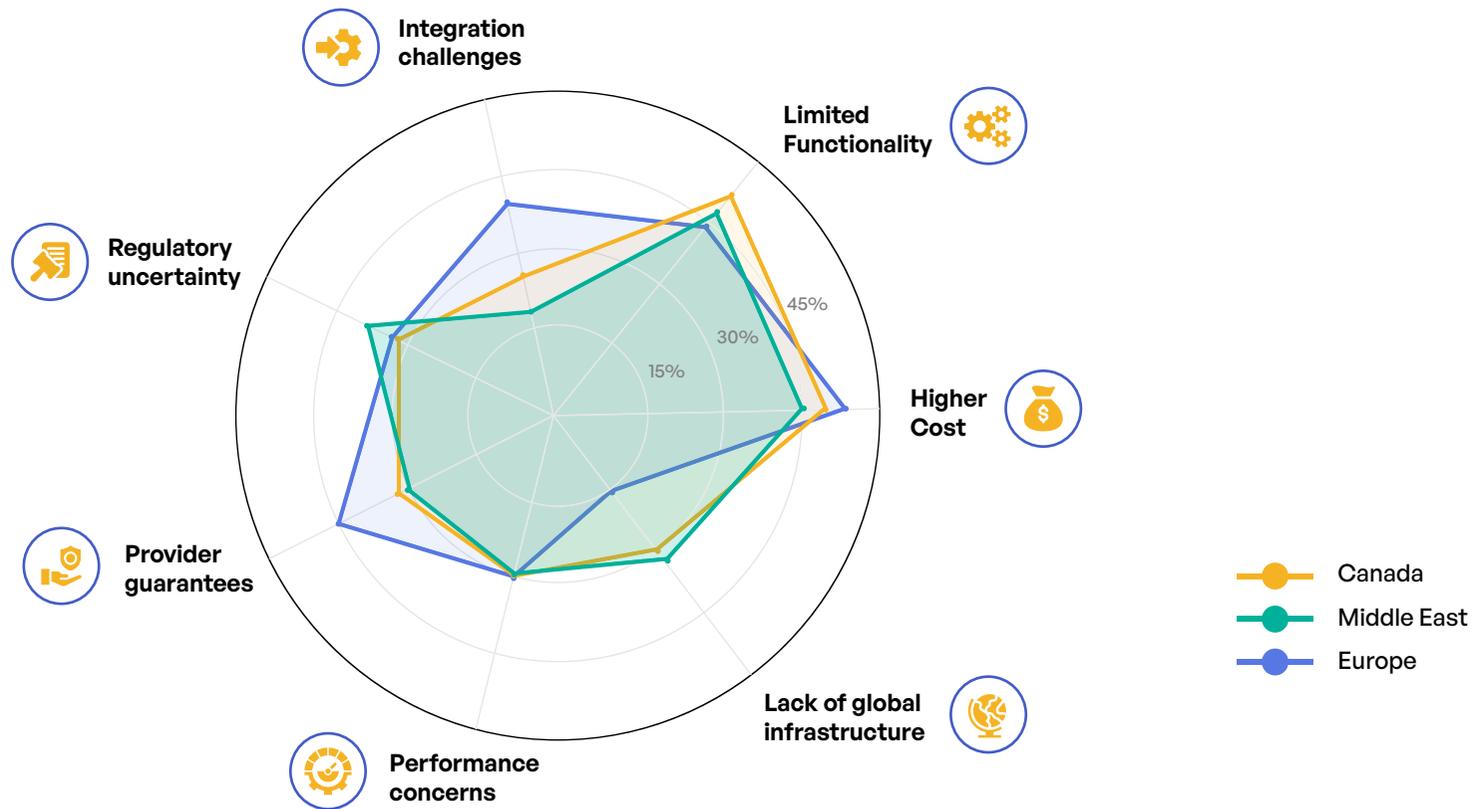


Figure 19: Barriers to adopting regional cloud providers, by region (directional estimates)

Europe's barrier profile peaks on higher costs and concerns over provider sovereignty guarantees. **The provider guarantee concern is among the most region-specific findings in the dataset.** It reflects growing unease about whether cloud providers, particularly U.S.-headquartered ones, can deliver on sovereignty promises when subject to laws like the U.S. CLOUD Act. Europe also leads on integration challenges, likely because mature IT infrastructure creates more friction when migrating to regional alternatives.

Canada's barrier profile is shaped by limited local alternatives and functionality concerns. Canadian organizations appear to find that domestic or regional cloud offerings don't match the feature sets of global hyperscalers. The cost barrier is also elevated, and regulatory uncertainty is the lowest of the three regions, fitting Canada's well-established PIPEDA context.

The Transparency Gap Is the Hidden Sovereignty Problem

A major sovereignty risk is visibility. In a 2025 survey of 2,000 European SMEs, 57% said they do not know whether their cloud provider guarantees EU-only storage. That uncertainty is already a stakeholder issue: 51% reported increased concern about data location, with customers and company directors most vocal. The same survey found 72% worry about data being stored in the United States, and 21% are considering switching providers due to geopolitical and economic concerns. The message: Sovereignty now includes provider assurances that business leaders can verify.⁵



The Middle East presents the most distinctive shape. **Regulatory uncertainty is the highest at approximately 37%**, reflecting the rapid pace of change under PDPL and SDAIA. Lack of global infrastructure scores highest of any region, pointing to the practical challenge of building sovereign cloud capacity in a region that has historically relied on international providers. Integration challenges are notably the lowest, which makes sense given that many Middle Eastern organizations are building new infrastructure rather than retrofitting legacy systems.

On regulatory concerns, the region-specific questions reveal sharp differences. Europe's top two concerns are the EU AI Act (40%) and geopolitical shifts related to U.S. policy (36%). Canada's attention is on changes to U.S. data-sharing arrangements (40%) and the CLOUD Act (21%). The Middle East is focused on implementing new data protection laws (37%) and geopolitical instability (33%). Each region faces a fundamentally different set of pressures, which means a one-size-fits-all sovereignty strategy is unlikely to work for any organization operating across multiple regions.

Taken together, the cross-analyses reveal that sovereignty is not experienced uniformly. Industry, role, size, and geography all shape how organizations understand, encounter, invest in, and plan for sovereignty requirements. The most capable organizations tend to be large, security-focused, and in regulated industries. The most vulnerable tend to be smaller, less aware, and operating in regions where the regulatory ground is still shifting.

Deeper Cross-Analyses: Compliance, Jurisdictional Reach, and AI Governance

The four cross-analyses above cut across the most visible dimensions: industry, role, size, and region. But the survey data supports three additional angles that deepen the picture. These examine how compliance maturity correlates with outcomes, whether jurisdictional complexity amplifies risk, and whether AI governance practices show any relationship to incident rates. Each draws on columns and crosstabs that go beyond the primary demographic breakdowns.

Compliance maturity does not fully insulate organizations from incidents. The survey included regulatory impact matrices for each region—PIPEDA in Canada, PDPL and SDAIA in the Middle East, and GDPR, the Data Act, and the AI Act in Europe. These allow a rough proxy for compliance maturity: Respondents who report higher regulatory impact and full compliance should, in theory, experience fewer incidents. The data partially supports this but with an important caveat.

In Canada, where 79% of respondents report full PIPEDA compliance, the incident rate is the lowest of the three regions at 23%. In Europe, where GDPR is well established and respondents report high familiarity, incidents sit at 32%. But the Middle East—where 93% say PDPL and SDAIA directly impact their operations—reports the highest incident rate at 44%. The disconnect is telling. High reported regulatory impact does not automatically translate into lower incident rates. What it may instead reflect is

that newer regulatory environments create a compliance-awareness gap: Organizations know the rules have changed but have not yet built the operational infrastructure to enforce them consistently.

On the benefits side, the pattern is more encouraging. Regions with higher reported compliance maturity also show stronger benefit perception. Europe leads on data governance as a perceived benefit (42%), and Canada leads on reduced legal risks alongside its high PIPEDA compliance rate. This suggests that while compliance maturity does not eliminate incidents, it does correlate with the ability to extract strategic value from sovereignty investments—a finding that reinforces the case for sustained compliance effort even in the face of persistent operational risk.

Jurisdictional complexity amplifies incident exposure. Each regional survey asked respondents to identify the provinces, countries, or EU member states in which their organizations operate. While these columns differ across the three surveys, they share a common analytical structure: Respondents who operate across more jurisdictions face more sovereignty friction.

The pattern is visible in the industry data. Financial Services—a sector that almost always operates across multiple jurisdictions—reports a 34% incident rate with the heaviest compliance spending. Manufacturing, which frequently manages cross-border supply chains, reports the highest incident rate of any sector at 52%. Technology and Software, despite its high awareness (48% "very well informed"), reports 33% incidents—close to the aggregate—likely because its cloud-native model creates broad but relatively uniform jurisdictional exposure.



The size data provides another lens. Organizations with over 20,000 employees—which almost always span multiple jurisdictions—report a 45% incident rate, compared to 28% for those with 500 to 999 employees. When combined with the finding that 41% of Middle Eastern respondents select cross-border transfer assessments as a top resource need (compared to 35% in Europe and 37% aggregate), the picture becomes clear: Every additional jurisdiction an organization touches adds a layer of compliance complexity, and that complexity shows up in both incident rates and resource demands. Organizations expanding into new regions should model sovereignty costs per jurisdiction rather than treating compliance as a flat overhead.

Organizations with stronger AI safeguards report different incident profiles. AI governance is one of the newest dimensions of data sovereignty, and the survey data offers an early signal about whether safeguard adoption correlates with outcomes. Fifty percent of respondents report conducting regular AI audits, 48% perform impact assessments for high-risk AI, and 46% have consent management systems in place. Only 5% report no safeguards at all.

Financial Services, the sector with the highest AI audit adoption at 59%, reports a 34% incident rate—lower than Manufacturing (52%) and close to Technology (33%), despite handling some of the most sensitive data in the economy. Government and Public Sector organizations, which lead on AI data localization at 36%, report 27% incidents. While correlation is not causation, the pattern is directionally consistent: Sectors that have invested most heavily in AI governance practices report incident rates at or below the aggregate average of 33%.

The management approach data adds nuance. Organizations that keep all AI training data in their home region (36% of the sample) are disproportionately in Government and regulated sectors with lower incident rates. Those using a mixed approach based on data sensitivity (34%) span a wider range of incident outcomes, depending on how rigorously "sensitivity" is defined and enforced. The 21% still developing their AI data policy represent a clear risk group—these organizations lack the framework to make consistent localization decisions, and as the EU AI Act and SDAIA requirements tighten, that gap will become an enforcement liability.

Together, these three deeper cross-analyses reinforce a common theme: Awareness and stated compliance are necessary but not sufficient. What separates lower-incident organizations from higher-incident ones is operational depth—the number of jurisdictions they can manage consistently, the maturity of their compliance infrastructure, and the rigor of their AI governance practices. These are the factors that determine whether sovereignty translates into protection or remains a compliance checkbox.

Implications and Recommendations

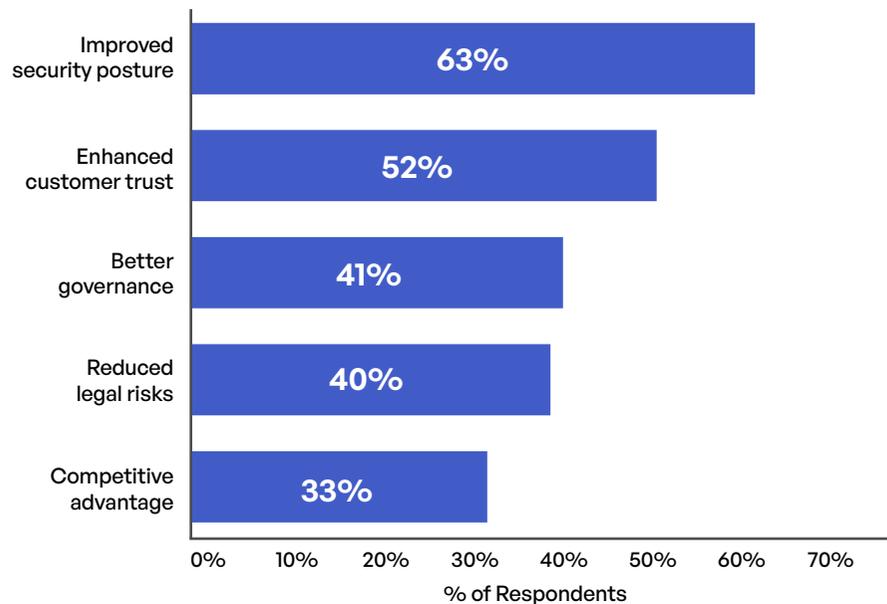
Business and Strategic Implications

The data points to a clear conclusion: Data sovereignty is delivering real value to the organizations that invest in it, but those investments are substantial and unevenly distributed. The tension between benefits and burdens defines the current moment.

On the benefit side, the numbers are hard to argue with. Nearly two-thirds of respondents (63%) associate sovereignty compliance with improved security posture, and more than half (52%) say it has strengthened customer trust. **These are broad-based gains that touch security, governance, legal risk, and competitive positioning simultaneously.**

Data Sovereignty: Benefits Realized vs. Resource Demands

Top Benefits Realized



Top Resource Drains

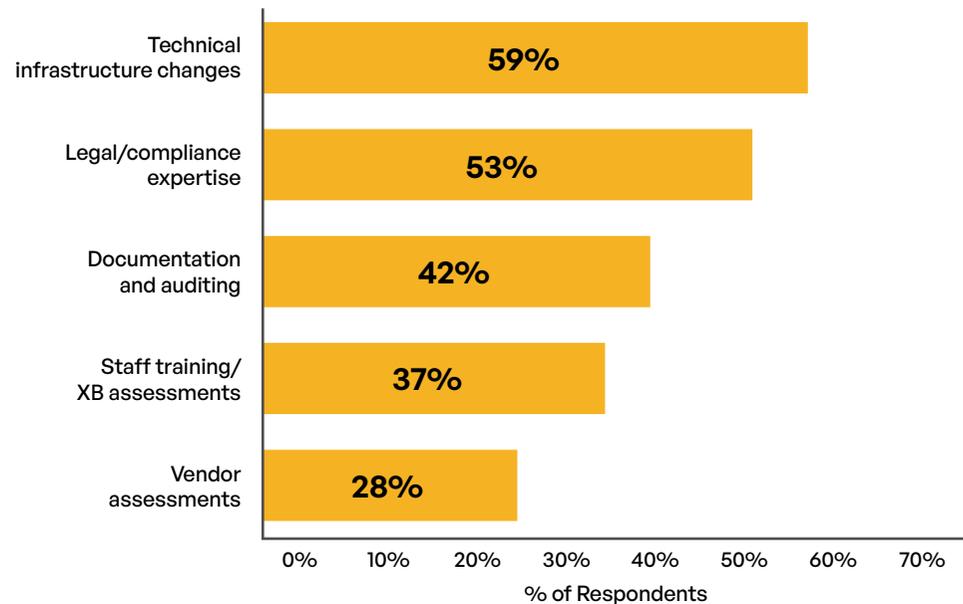


Figure 20: Side-by-side comparison of the top benefits realized and top resource demands





On the burden side, the picture is equally clear. Technical infrastructure changes consume the most resources at 59%, and legal expertise follows at 53%. For the largest organizations, spending in the top local-currency tier exceeds 45%. These are not one-time costs. Sovereignty compliance is an ongoing operational commitment that requires sustained investment in technology, people, and process.

The strategic implications break along three fault lines. **First, regulated industries are out front.** Manufacturing and Financial Services report the highest incident rates but also the strongest perceived benefits. Their practices around AI audits (59% in Financial Services) and data localization (36% in Government) can serve as models for less mature sectors.

Second, smaller organizations are falling behind. The 15-to-25-point gap between the smallest and largest organizations on nearly every measure is not sustainable as enforcement pressure increases. Without targeted support, this gap will widen.

Third, sovereignty knowledge is concentrated in security roles. The awareness gap between security-focused roles and IT implementation roles means that the people closest to implementation often lack the regulatory understanding needed to make informed decisions.

Importantly, sovereignty does not have to mean isolation. The survey data shows that day-to-day tools like email and cloud file sharing are largely manageable under sovereignty constraints, with the real complexity concentrated in infrastructure redesign, vendor compliance, and cross-border assessments. The goal is controlled collaboration, not blanket restriction. Organizations that build sovereignty into the architecture of how they share and move data—rather than simply locking it down—will preserve the speed and cross-border agility their operations depend on.

Policy and Operational Recommendations

Based on the patterns across all 286 responses, five recommendations emerge. Each is grounded in a specific finding from the data.



Recommendation 1: Prioritize compliance automation, especially for large and mid-sized organizations.

Automation is already the top planned strategy at 53% overall, and 69% of organizations with more than 20,000 employees intend to invest in it. Organizations that face the heaviest compliance burdens stand to gain the most from automating documentation, monitoring, and reporting workflows.



Recommendation 2: Adopt a localization-first approach for AI training data, particularly in government and healthcare. Government organizations already lead on AI data localization, and localized AI strategies correlate with stronger sovereignty postures overall. As the EU AI Act took effect in August 2025, organizations that have localized their AI data are better positioned.



Recommendation 3: Invest in sovereignty training for IT managers and specialists. This is the single largest role group at 42% of respondents, and their awareness trails security-focused roles on key sovereignty dimensions. Targeted training programs and cross-functional workshops with security teams could help close this gap.



Recommendation 4: Address cost and functionality barriers to regional cloud adoption through ecosystem development. Higher costs are the top barrier in Europe and a close second in Canada and the Middle East. Regional cloud providers, industry associations, and policymakers have a shared interest in developing sovereign cloud ecosystems that offer competitive pricing, enterprise-grade features, and credible sovereignty guarantees.



Recommendation 5: Build regulatory monitoring capacity for the AI Act, Data Act, and evolving cross-border frameworks. Forty percent of European respondents cite the EU AI Act as a top concern, 40% of Canadian respondents point to U.S. data-sharing changes, and 37% of Middle Eastern respondents are watching new data protection laws. Organizations need dedicated monitoring functions to track regulatory developments and translate them into operational adjustments before enforcement deadlines hit.

Recommendation Priorities: Data-Backed Action Items

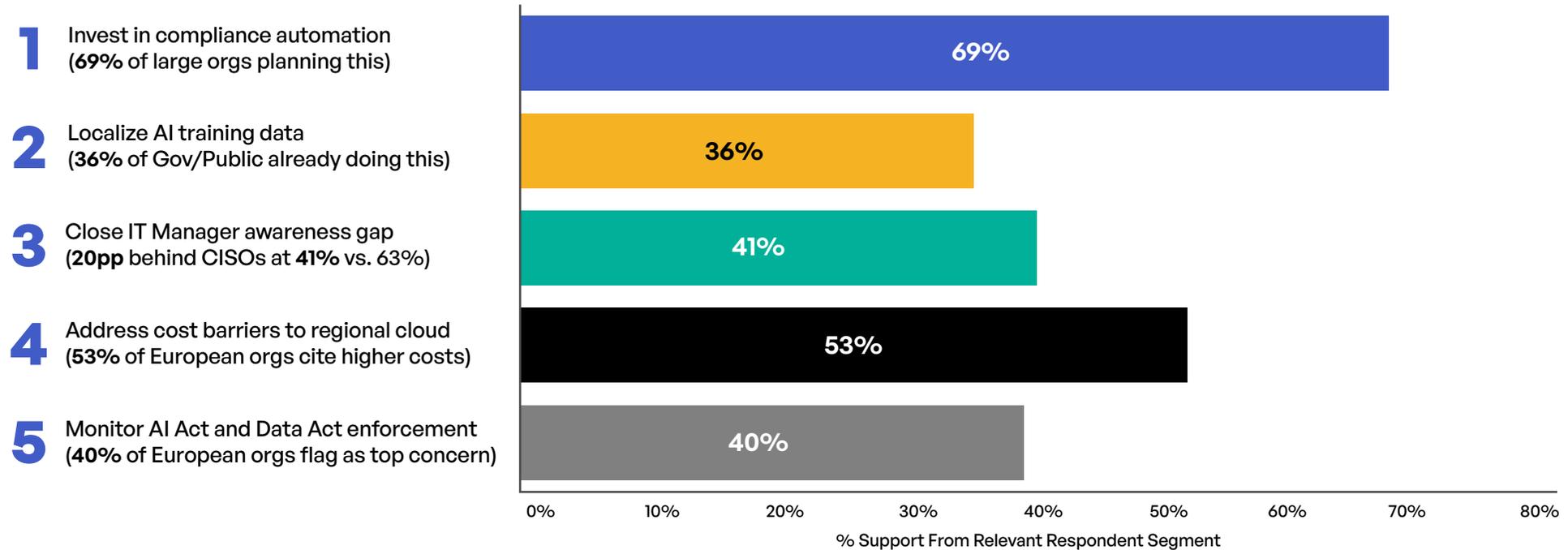


Figure 21: Five data-backed recommendations, each anchored to a specific survey finding

Sovereignty Readiness Checklist

The five recommendations above provide strategic direction. The checklist below translates them into an operational starting point. It is designed for security, IT, and compliance leaders who need to assess their organization’s current sovereignty posture and identify the most immediate gaps.

- Scope: Define what must remain sovereign.** Identify the specific data categories, workflows, and systems that fall under sovereignty requirements in each jurisdiction where you operate. Not everything needs the same level of control. Start with regulated data (personal data, financial records, health information) and expand from there based on contractual obligations and risk appetite.

- 2** | **Jurisdiction exposure: Map where provider and legal reach introduces risk.** For every cloud service, SaaS platform, and third-party processor in your stack, determine the legal jurisdiction of the provider, the physical location of data at rest, and whether foreign government access laws (such as the U.S. CLOUD Act or equivalent) could override local protections. This is where the 44% provider-guarantee concern flagged by European respondents becomes operational.
- 3** | **Control stack: Verify that technical controls enforce residency and access.** Sovereignty requires more than policy. It requires architecture. Confirm that data residency is enforced at the infrastructure level, that encryption key custody remains within your jurisdiction, and that access controls prevent unauthorized cross-border movement. The 59% of respondents who cite technical infrastructure as their top resource drain are working on exactly this layer.
- 4** | **Evidence pack: Prepare what you can produce in an audit or customer review.** Regulators, customers, and partners increasingly want proof, not assurances. Build an exportable evidence package that includes data residency logs, access audit trails, cross-border transfer documentation, and incident response records. The shift from “we believe we’re compliant” to “we can demonstrate compliance” is where implementation maturity becomes tangible.
- 5** | **Incident drills: Test your response to third-party failures and cross-border transfer events.** With 17% of respondents reporting third-party compliance failures and 12% reporting unauthorized cross-border transfers, these are not edge cases. Run tabletop exercises that simulate a vendor sovereignty breach, a government data access request, and an unauthorized transfer event. Identify who owns the response, what documentation is required, and how quickly you can contain the impact.

This checklist is not exhaustive, but it covers the five areas where the survey data shows the greatest gap between stated awareness and operational readiness. Organizations that can answer confidently on all five are well positioned. Those that cannot have a clear set of priorities to address.

Conclusion

Data sovereignty is no longer emerging. It has arrived. Across Canada, the Middle East, and Europe, the 286 professionals surveyed for this report paint a picture of a discipline that has moved from regulatory theory into operational reality, complete with measurable benefits, quantifiable costs, and incident rates that confirm the risks are not hypothetical.

The headline numbers tell a story of growing maturity alongside persistent gaps. **Four in five respondents (80%) feel well or very well informed about sovereignty requirements. Nearly two-thirds (63%) associate compliance with improved security. More than half plan to invest in compliance automation over the next two years.** These are not the numbers of an industry struggling to understand sovereignty. They are the numbers of an industry grappling with the complexity of doing it well.

But the gaps matter just as much as the gains. One in three organizations experienced a sovereignty-related incident in the past year, and in the Middle East that figure rises to 44%. A meaningful awareness divide persists between security leaders and IT implementers. Smaller organizations trail their larger counterparts by 15 to 25 points on awareness, spending, and planning. And each region faces a different set of barriers: Europe is wrestling with provider trust and layered regulation, Canada with limited local alternatives and U.S. data-sharing uncertainty, and the Middle East with regulatory newness and infrastructure gaps.

What this data ultimately suggests is that sovereignty is becoming a differentiator. Organizations that invest deliberately—in automation, in training, in regional infrastructure, and in regulatory monitoring—are seeing returns that go well beyond compliance. They are building stronger security postures, deeper customer trust, and more resilient operating models. Those that underinvest, whether by choice or constraint, face growing exposure to incidents, fines, and competitive disadvantage.

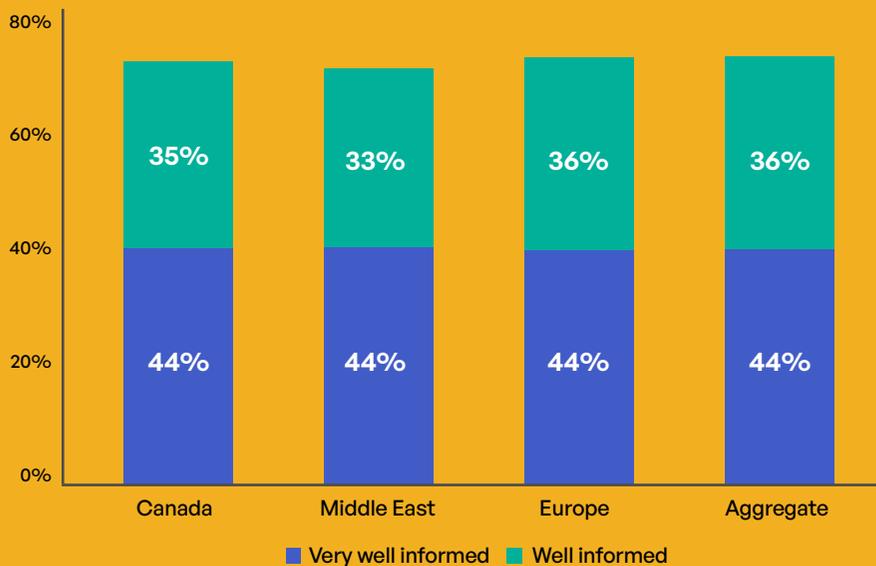
The regulatory trajectory is clear. The EU AI Act and Data Act add new layers of obligation in Europe. Cross-border data-sharing tensions between Canada and the United States show no signs of easing. The Middle East's regulatory landscape will continue to mature and tighten. For organizations operating across any of these regions, the question is no longer whether to invest in sovereignty but how much, how fast, and where to start.

This report has aimed to answer those questions with data rather than opinion. The survey findings, the cross-analyses, and the recommendations above are designed to give decision-makers a clear, evidence-based foundation for their next moves. Sovereignty is a long game, and the organizations that treat it as one will be the ones best positioned when the next wave of regulation arrives.

Across all three regions, the practical shift is from stated compliance to provable control. With one in three respondents reporting a sovereignty-related incident in the past year, and the Middle East reaching 44%, the standard is no longer “we believe we’re compliant”—it’s “we can show where data resides, how access is governed, and how cross-border movement is prevented or documented.” Organizations that treat sovereignty as an evidence discipline—supported by automation, repeatable controls, and audit-ready documentation—will be the ones that reduce incidents while preserving speed and cross-border collaboration.

Data Sovereignty Trends Dashboard: Key Metrics at a Glance

A. Sovereignty Understanding



B. Incidents Reported (% "Yes")

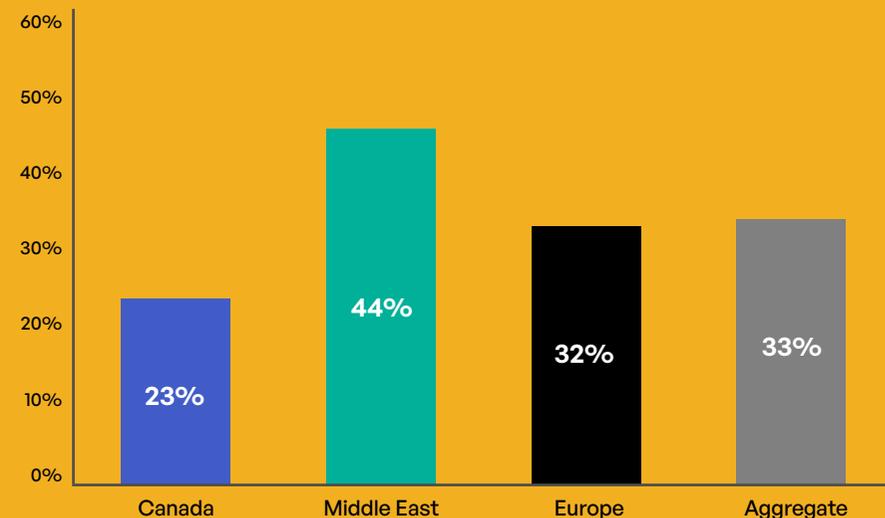


Figure 22A: Data sovereignty trends dashboard – key metrics at a glance

C. Top Business Benefits



D. Planned Strategies (Next 2 Years)

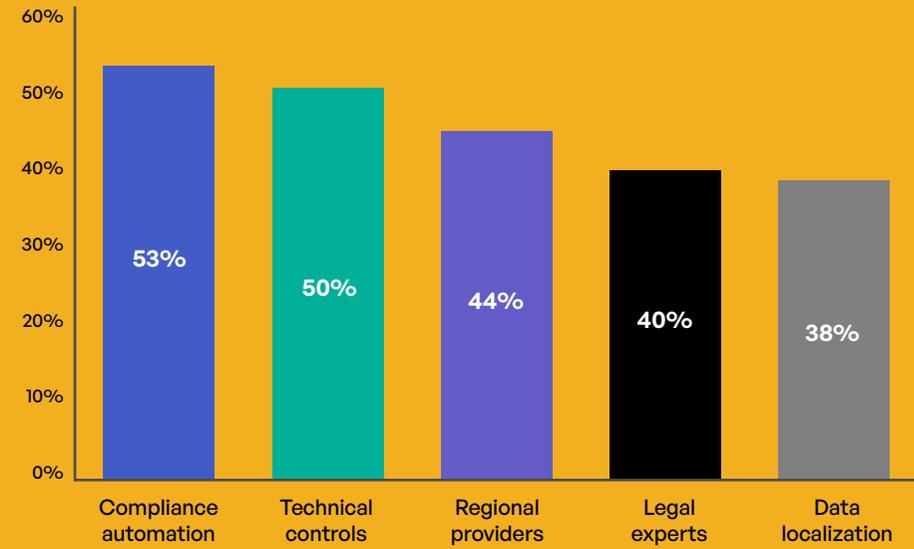


Figure 22B: Data sovereignty trends dashboard – key metrics at a glance

Kiteworks and Data Sovereignty

This report identifies a consistent pattern across all three regions: Awareness is high, but incidents persist because the gap between stated compliance and provable control remains open. Closing that gap requires architecture, not just policy — controls that enforce residency and access at the infrastructure level, evidence artifacts that satisfy regulators and customers on demand, and response readiness that has been tested before the incident arrives. The Kiteworks Private Data Network is purpose-built for this challenge. Its flexible deployment options — on-premises, private cloud, hybrid, and FedRAMP — allow organizations to store sensitive content within their home jurisdiction, whether that is Canada, the Middle East, or the EU.

Kiteworks retains encryption key custody in-jurisdiction, enforces geofencing through configurable IP controls, and consolidates email, file sharing, managed file transfer, SFTP, and data forms into a single zero-trust platform where every file is controlled, tracked, and protected across its entire life cycle. Its centralized, immutable audit logs and automated compliance reporting — with preconfigured templates for GDPR, DORA, NIS 2, PIPEDA, PDPL, and more — deliver the exportable evidence that this report identifies as the operational differentiator between organizations that experience incidents and those that prevent them. In a landscape where 59% cite technical infrastructure as the top resource drain and 55% plan to invest in compliance automation.

Kiteworks replaces fragmented point solutions with a unified governance framework that reduces complexity while producing the audit-ready documentation regulators, auditors, and enterprise customers increasingly demand.

Legal Disclaimer

Legal Disclaimer The information provided in this report is for general informational purposes only and should not be construed as professional advice. Kiteworks and Centiment make no representations or warranties of any kind, express or implied, about the completeness, accuracy, reliability, suitability, or availability of the information contained in this report. Any reliance you place on such information is strictly at your own risk. None of the sponsoring or contributing organizations shall be liable for any loss or damage including without limitation, indirect or consequential loss or damage, or any loss or damage whatsoever arising from loss of data or profits arising out of, or in connection with, the use of this report. Readers should consult with qualified legal counsel and cybersecurity professionals when addressing specific compliance requirements. The data in this report was analyzed using AI and the content was generated with AI assistance. While AI enhances analytical capabilities, it can occasionally produce errors or biased information that should be considered when reviewing these findings.

About Centiment

Centiment is a market research firm specializing in data collection and analysis for the cybersecurity and technology sectors. The company delivers actionable insights through customized survey design, targeted respondent recruitment, and sophisticated analytics. Centiment's proprietary research platform ensures exceptional data quality through AI-driven verification and expert human oversight. The company serves Fortune 500 enterprises, technology vendors, and government agencies, providing intelligence for strategic decisions in evolving markets. Headquartered in Denver, Centiment conducts research globally to help organizations understand complex technology landscapes and cybersecurity trends.

References

¹“Digital Sovereignty in Europe in 2025: What’s ‘Plan B’?” IDC, August 27, 2025, <https://www.idc.com/resource-center/blog/digital-sovereignty-in-europe-in-2025-whats-plan-b/>.

²“First administrative monetary penalty issued under Ontario’s health privacy law,” Privacy Transparency Empowerment, September 2, 2025, <https://www.ipc.on.ca/en/resources/first-administrative-monetary-penalty-issued-under-ontarios-health-privacy-law>.

³Richard Speed, “Canadian data order risks blowing a hole in EU sovereignty,” The Register, November 27, 2025, https://www.theregister.com/2025/11/27/canada_court_ovh.

⁴Alexander Baghal-Schmid and Luiza Esser, “What has happened so far, expressed in numbers,” CMS, May 13, 2025, <https://cms.law/en/int/publication/gdpr-enforcement-tracker-report/numbers-and-figures>.

⁵“European SMEs seek greater Data Sovereignty amid rising trust concerns, reveals team.blue report,” team.blue, July 24, 2025, <https://press.team.blue/252488-european-smes-seek-greater-data-sovereignty-amid-rising-trust-concerns-reveals-team-blue-report/>.