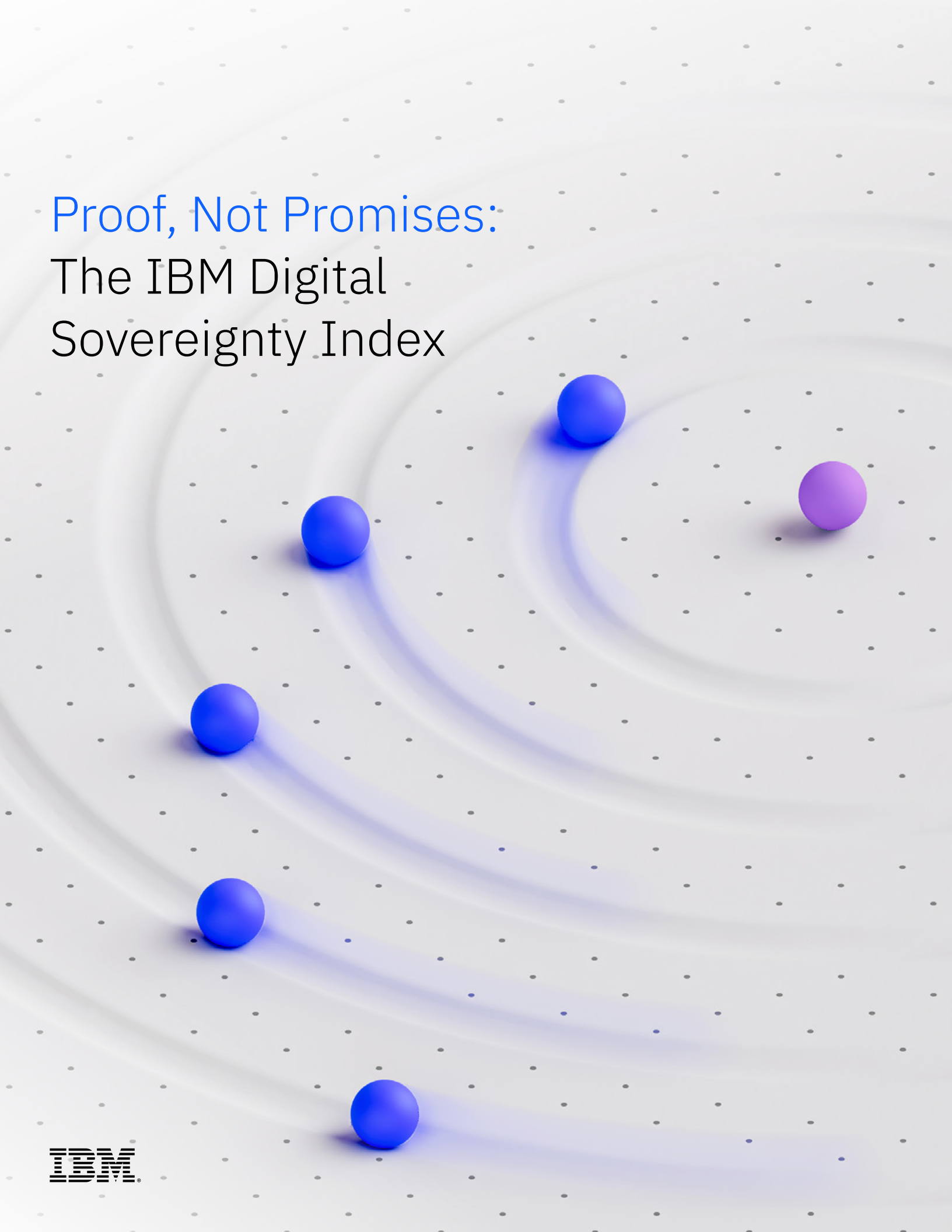
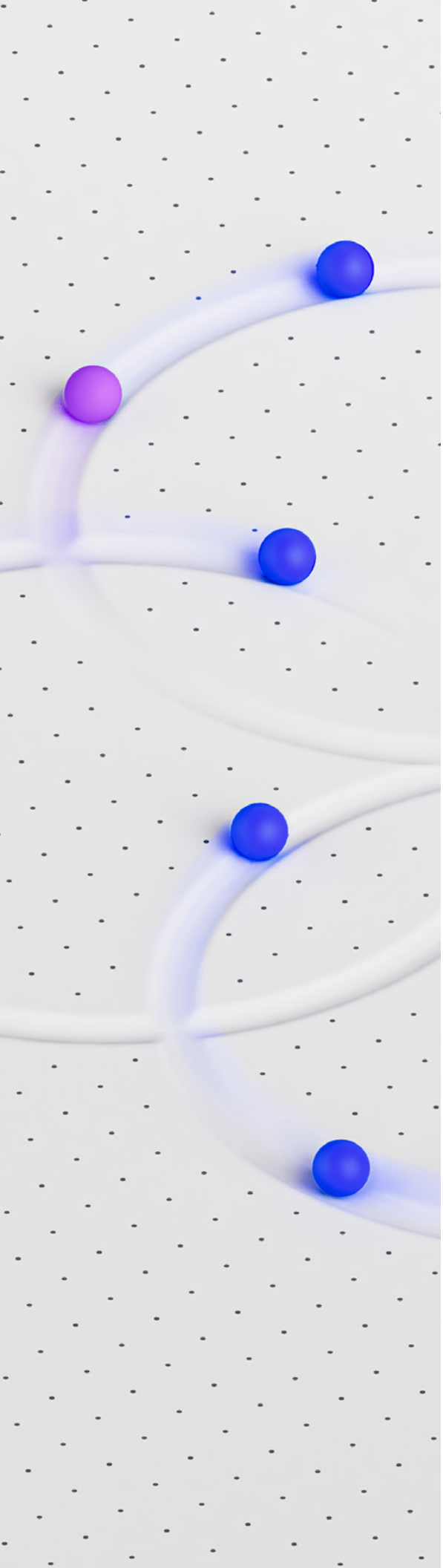
Proof, Not Promises:
The IBM Digital Sovereignty Index





Contents

Foreword 3
By Jonathan Adashek
Senior Vice President
Chief Global Affairs Officer, IBM

Executive Summary 4

Chapter one 6
Having control is one thing. Proving it is another.

Chapter two 11
The IBM Digital Sovereignty Index

Chapter three 19
IBM Perspective: A new operating model

Chapter four 23
The leadership imperative

Further information and resources 27

Methodology 28



Foreword

Jonathan Adashek
Senior Vice President, Chief Global Affairs Officer, IBM

Technology has become a geopolitical variable. We have seen decisions once driven primarily by cost, capability, and efficiency increasingly being shaped by questions of resilience, dependency, and national interest. For organizations around the world, this is creating new demands for control and accountability.

Digital sovereignty is one of the most pressing topics we see tied to these challenges. IBM's first of its kind Digital Sovereignty Index looks at how prepared organizations are to demonstrate authority over their technology, data, operations, and AI.

The regulators, policymakers and public-sector officials interviewed for this report described growing expectations for organizations to demonstrate control and show evidence that it works as intended. In our view, this makes governance an operational discipline, embedded in how systems are designed, managed, and monitored daily. It is more important than ever that control and independence are built into architecture, regardless of specific technology choices.

Organizations can no longer afford to assume they are in control until they are forced to act. Failing to prepare can limit flexibility and choice and cause business disruptions when conditions change or when scrutiny arrives.

AI is only accelerating this challenge. As organizations adopt increasingly powerful systems, questions of accountability, traceability, and control are becoming more urgent and more complex.

IBM has for more than a century operated with a simple belief: openness enables scale, innovation, and resilience. That principle is becoming even more important in the AI era. Unlike previous generations of technology, AI introduces new questions of transparency and control that extend beyond infrastructure. Over-reliance on a single provider or model can erode flexibility and concentrate risk precisely when organizations need greater freedom of action and greater accountability.

Business leaders must operationalize proof, while policymakers establish clear, outcome-based frameworks. Together, they can make digital sovereignty an ongoing discipline, rather than a reaction to the next organizational crisis.

Ultimately, digital sovereignty is not defined by what organizations say they control, but by what they can demonstrate when challenged. We hope this report provides a useful perspective on what it takes to close that gap, and how we all can learn from those organizations adapting best to the age of sovereign systems.

Executive Summary

Digital sovereignty challenges rarely announce themselves as such. More often, they arrive disguised as something else: a regulatory audit, an AI incident, a cyberattack, a provider outage, or a major technology change.

We found that the concept itself is not unfamiliar to executives. In fact, it has earned a place on the executive agenda, with a Suse survey indicating that many organizations are already pursuing a digital sovereignty strategy or expecting to have one in the near future.

More than nine in ten respondents aligned with our definition of digital sovereignty as: An organization's ability to retain control and provide credible evidence of that control across critical AI, technology, operations and data.

Retained control means remaining accountable for and in control of critical digital systems and decisions–including where third parties are involved–with the ability to set boundaries, reconstruct what happened, intervene, recover or change providers.

> Proof is not a single document or certification, but a body of evidence –including governance records, technical controls, audit trails and tested recovery or exit arrangements –that substantiates retained control.

Yet despite broad alignment with the concept, organizations tend to define sovereignty more narrowly in practice. Their instinctive understanding centers on data control, technology independence, resilience, and the freedom to make their own technology decisions. AI, operations, and the ability to prove control are far less prominent in how leaders think about sovereignty.

The urgency is growing as geopolitical uncertainty, evolving regulation, rapid AI adoption and dependence on globally distributed infrastructure reshape the conditions enterprises operate in. Changes in access to critical technology ecosystems can put an enterprise's ability to retain control and maintain operations to the test.

An operational, regulatory or technology issue can have a sovereignty dimension when it tests whether an enterprise retains the authority and practical ability to control its critical systems and decisions–including when external parties or restrictions constrain its options–and can demonstrate that control.

Increasingly, that means providing formal evidence to regulators, auditors, customers, boards, or other stakeholders. The research found that 94% of responding enterprises had experienced at least one sovereignty challenge in the previous three years. Among those enterprises, 91% were required to demonstrate control during their most testing event, while 81% had to provide formal evidence.

The scrutiny that follows is often practical rather than theoretical. Organizations can be asked to show who was accountable, what happened, whether controls worked as intended, whether decisions can be explained, and whether they can recover, adapt, or change course without disruption. Sovereignty is increasingly not just about the existence of controls but also the ability to produce credible evidence of them under pressure.

Drawing on a survey of 2,003 senior decision-makers within large enterprises across seven markets, alongside 25 policymaker and regulator interviews and perspectives from 17 senior

customer leaders, IBM's research underpins the inaugural IBM Digital Sovereignty Index, which benchmarks evidence maturity across AI, Technology, Operations and Data.

The Index reveals a significant contrast between confidence and evidence maturity. While an average of 82% of respondents were very or extremely confident they could provide evidence of control across six dimensions, only 26% of enterprises reached the Index's Leading maturity tier. Although these are different measures, they show that confidence runs ahead of the strongest evidence standards.

Most surveyed organizations focus on having control. Far fewer are prepared to prove that control quickly, credibly, and without disruption.

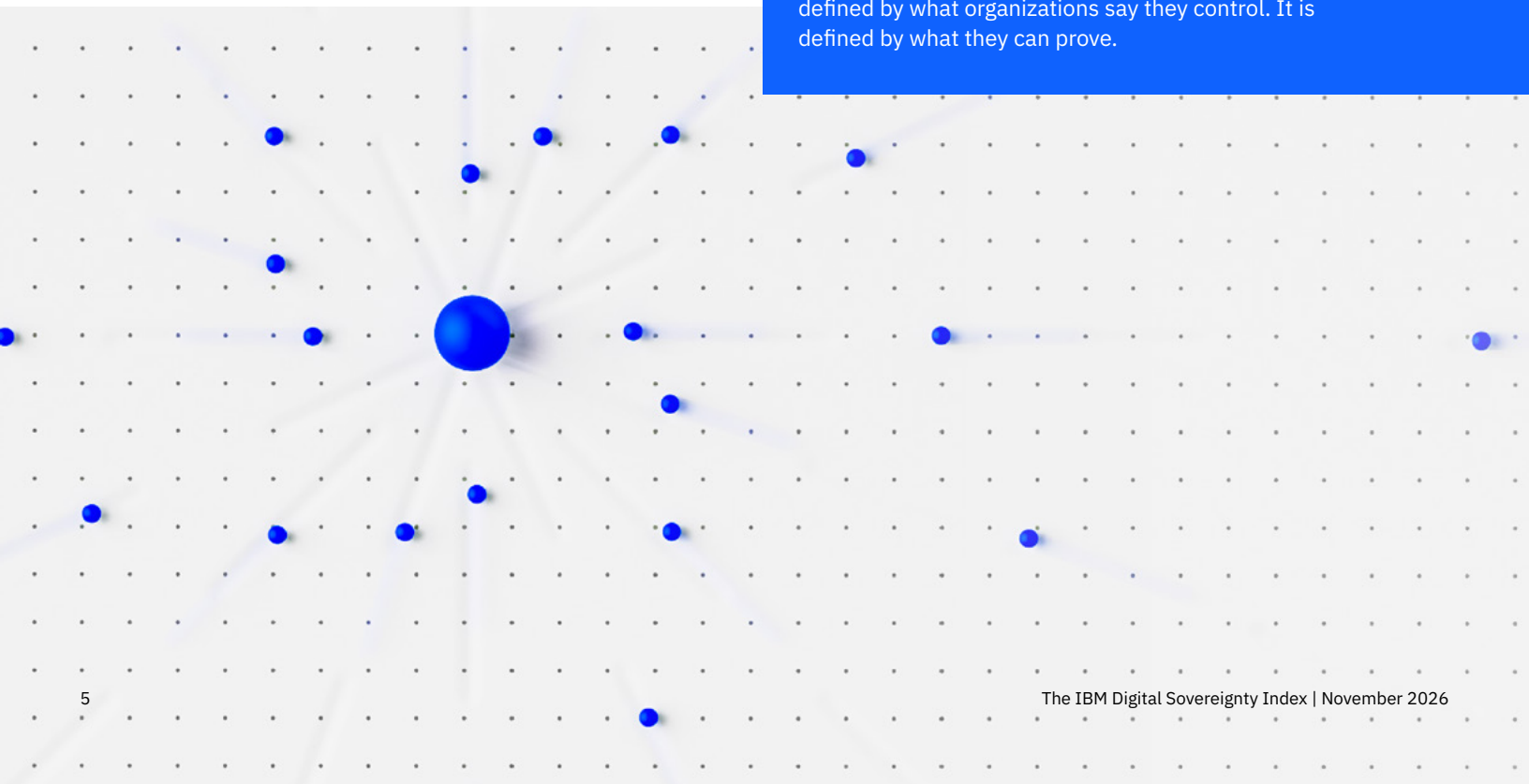
The findings suggest that many enterprises have governance structures and controls in place but struggle to assemble and produce the evidence needed when scrutiny arrives. The issue is not necessarily a lack of governance. The issue is whether governance can withstand scrutiny and whether evidence can be produced without significant friction, delay, or disruption to the business.

This challenge becomes even more acute as AI moves into core business operations. Enterprises must increasingly be able to explain where AI systems are operating, what they are doing, who authorized them, who remains accountable for their actions, and how the organization would respond if a critical provider or model failed. Yet our findings show that, for the enterprises surveyed, AI is simultaneously the most common sovereignty challenge and the area where evidence of control is least mature.

> Digital sovereignty, therefore, is no longer simply about having control. It is about being able to prove control when it matters most.

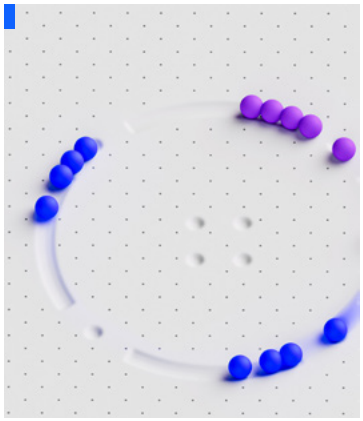
Because when the test comes, the difference between organizations that can demonstrate sovereignty and those that cannot is not theoretical. It is the difference between adapting with confidence and being forced into a costly scramble for evidence. It is the difference between strategic flexibility and operational disruption. Between retaining freedom of action and discovering, under pressure, that control was more fragile than it appeared.

In the new business environment, sovereignty is no longer defined by what organizations say they control. It is defined by what they can prove.



Chapter 1

Having control is one thing. Proving it is another.



“Digital sovereignty is not a compliance checkbox –it’s a business reality.”

Emmanuel Frenehard
Chief Digital Officer, Sanofi

Sovereignty challenges are already part of surveyed enterprises’ operational reality, while scrutiny of data, AI, technology and critical operations is increasing.

Critical business operations increasingly depend on cloud, AI, globally distributed infrastructure and external providers. Changes in regulation, geopolitical conditions or access to critical technologies can create a sovereignty challenge by affecting an enterprise’s ability to retain control and keep operating.

Governance establishes accountability and controls, while resilience supports continuity and recovery. Both contribute to digital sovereignty, but neither alone establishes whether an enterprise retains effective authority over its critical systems and can exercise that authority when external dependencies constrain its options.

The test is already here

We found that **94% of enterprises surveyed have experienced at least one sovereignty challenge in the past 3 years**–an event that put retained control, or the ability to demonstrate event that put retained control, or the ability to demonstrate it, under scrutiny. These included AI-related issues, cybersecurity incidents, regulatory events and significant provider changes.

Among those enterprises, **91%** were required to demonstrate that they retained control, while **81% had to provide formal evidence**[1]–for example to regulators, external auditors, customers or internal stakeholders.

This shows that the need to demonstrate control already commonly accompanies a sovereignty challenge, rather than being an exception.

Our research identified that demands for evidence can arrive while the enterprise is still trying to investigate, understand and respond to the underlying event. When this happens, proof has to be produced during the response itself, rather than as a separate exercise once the situation has been resolved.

[1] Formal evidence requests included external requests–for example from regulators, external auditors, customers, clients, citizens or independent assurance processes–and formal internal reviews, including board or executive review, internal audit, risk, compliance, legal or post-incident review. The 91% figure additionally includes informal requests for evidence or documentation.

Challenges do not remain neatly contained to a single area

Sovereignty challenges can extend beyond the technology environment. In respondents' most testing events, AI, Data and Operations were involved almost as frequently as Technology[2].

The operational significance is that no single function necessarily holds the whole answer. An AI-related challenge, for example, may require data lineage, technology records, governance evidence and an operational response–bringing several functions into the same investigation and requiring work from all of them to produce proof of sovereignty.

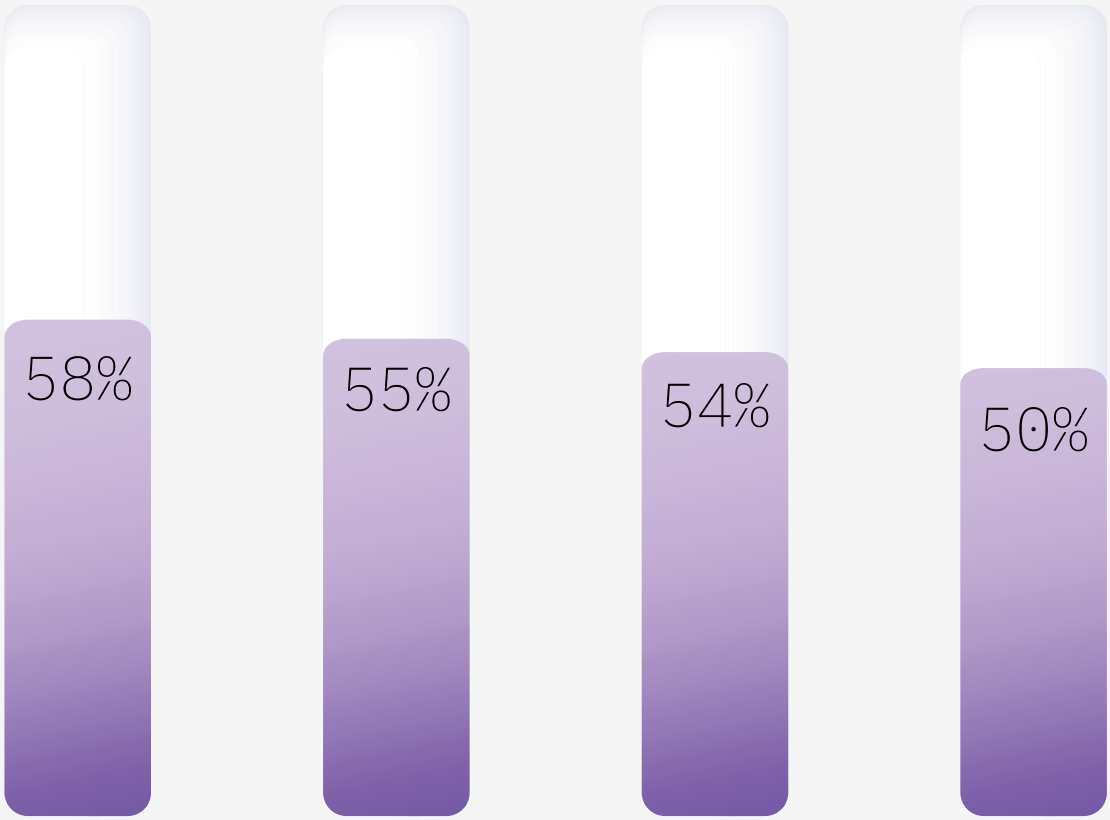
Understanding the burden of proof

What constitutes credible proof depends on the enterprise, the critical systems involved and the nature of the challenge. It may include evidence of accountability, traceable records, working controls, intervention and recovery capabilities, tested exit arrangements, and governance or assurance that can withstand scrutiny.

The enterprise might need to provide this evidence to regulators, auditors, customers or internal stakeholders, and it will need to withstand scrutiny both during routine governance and when an incident, disruption, migration or recovery event puts those arrangements to the test.

Area involved directly in the incident

FIGURE 1



Technology platforms, cloud infrastructure or providers

AI systems, models or AI-enabled decisions

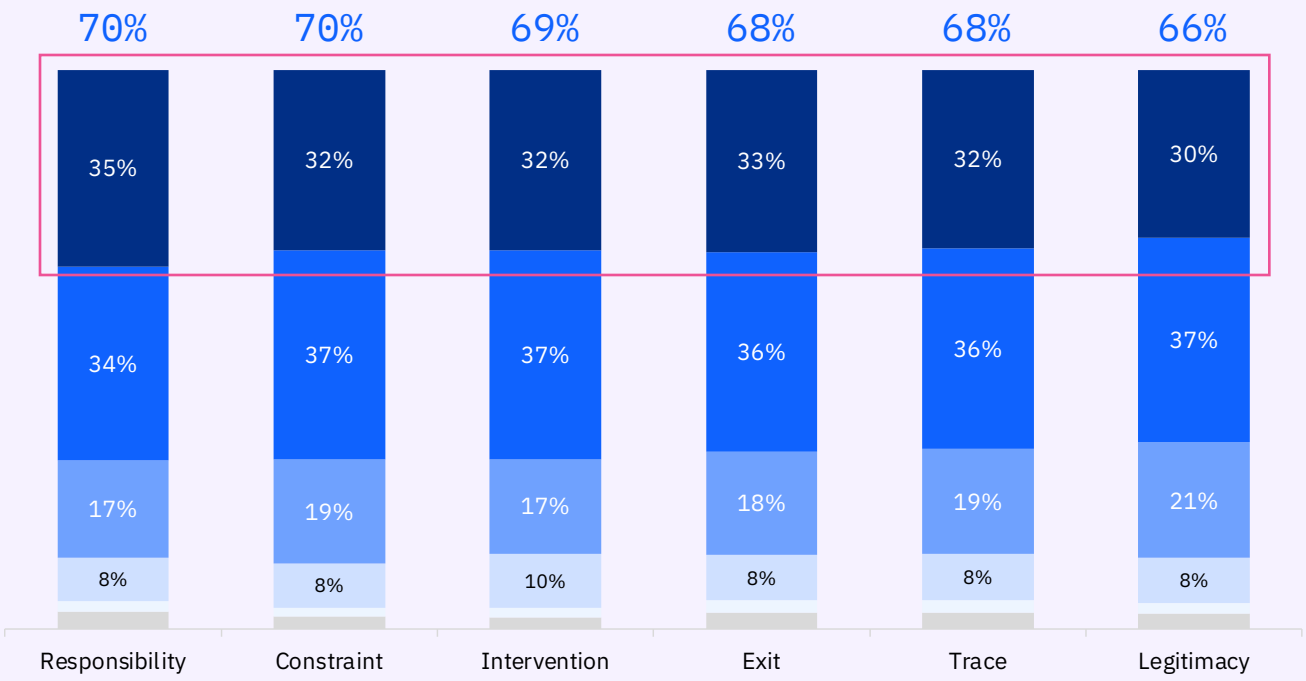
Data governance, data access, movement or use

Digital operations, business processes or service delivery

[2] Technology, AI, Data and Operations are the four enterprise pillars respondents were surveyed about. Respondents who had experienced a sovereignty challenge were asked which areas were involved in their most testing event. These areas were described as follows. Technology covers critical platforms, infrastructure and providers; AI covers AI systems, including models and AI-enabled business decisions; Data covers critical data assets; and Operations covers critical operational processes, including people, processes and governance.

Ability of organizations to demonstrate evidence

FIGURE 2



This is where the difficulty becomes apparent. Most enterprises surveyed (around seven in ten) can prove control of digital sovereignty when challenged. But **only around a third can do so fully and credibly, without significant follow-up.** Evidence may be dispersed across systems, teams and providers, requiring additional effort to assemble and validate–restricting the ability to change course precisely when the enterprise is already under pressure and needs to act.

An enterprise may have governance and controls around an AI system yet struggle to produce a clear record of which model and data were used, what controls applied and who was accountable for a decision. Or it may have a contractual right to exit a critical provider without being able to demonstrate that workloads, data and controls can be moved while maintaining business continuity.

For example, consider a theoretical scenario where a bank's AI-assisted lending system produces questionable decisions after its cloud provider rolls back a model. The bank has governance arrangements and contractual rights, but the records needed to establish what changed, which model ran and who could intervene are spread across its own systems and those of the provider.

Facing regulatory scrutiny, the bank pauses planned updates to the affected service while teams reconstruct the evidence. Engineers who would otherwise be delivering improvements are diverted into the investigation. Even if the bank ultimately demonstrates that it retained control, the time spent proving it has delayed new releases and put innovation on hold.

Proof should therefore be understood as a capability in its own right: the ability to show which person or team had authority, what controls were operating and what happened when those controls were tested.



"Because they are able to cope with the issue, people say 'we have everything under control.' But the real question is: why can't we produce proof immediately after the incident? In many cases, it takes months and can bring critical business updates to a standstill, especially in heavily regulated industries."

Dennis Lauwers, VP and CTO
Sovereign Technologies and Hybrid Automation, EMEA, IBM

FIGURE 3



> “As organisations embed AI more deeply into their operations, data sovereignty must be more than a matter of confidence. Organisations need to be able to demonstrate where their data comes from, how it can be used, and what controls are in place. Trusted, well-governed data from established providers enables businesses to continue innovating securely and responsibly.”
>
> **Debbie Lawrence**
> Group Head of Data Strategy and Management, LSEG

Most surveyed enterprises retain control but doing so comes at a cost

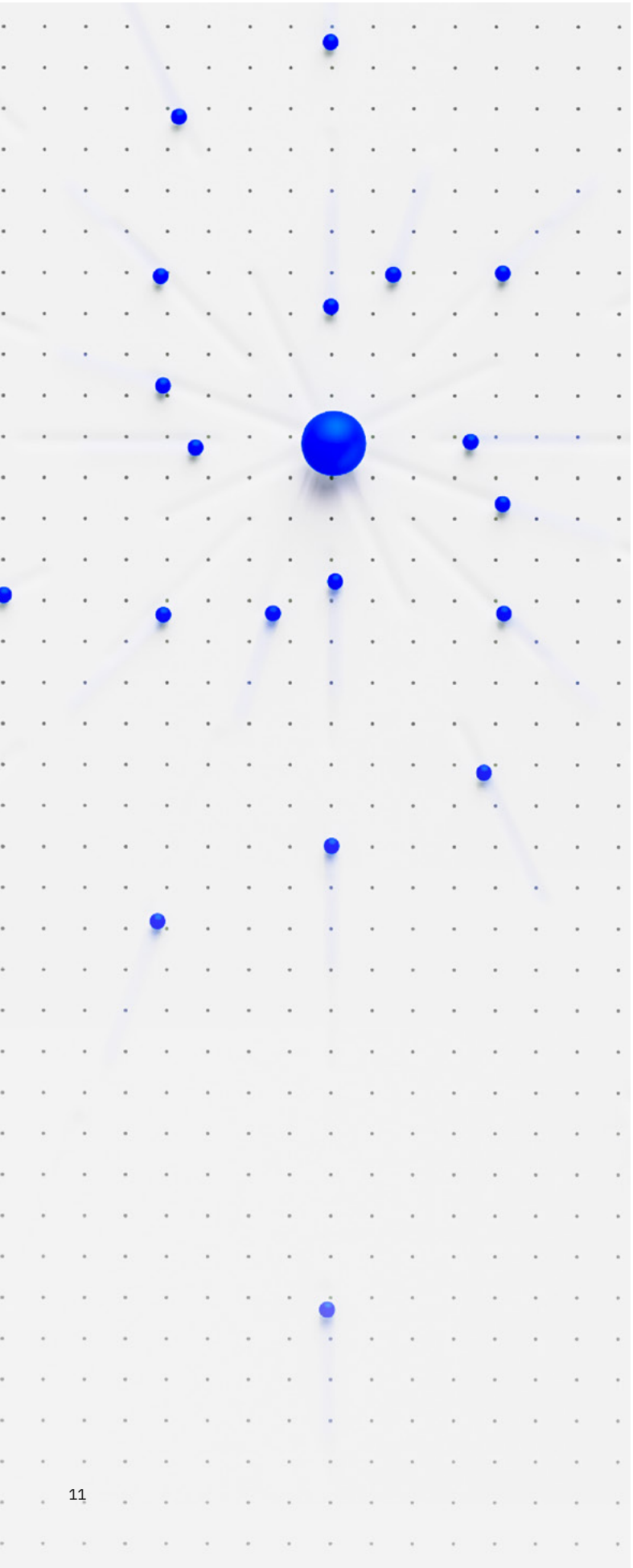
Most responding enterprises demonstrated resilience when sovereignty was challenged: **62%** retained control during their most testing event. Yet only **30%** resolved the situation without material disruption[3]. A further **32%** retained control but required significant manual effort or coordination, while **20%** experienced disruption or delay before recovering without major long-term impact. **Another 11% reported having to change a provider, architecture, AI use case, data practice or operating process.**

These findings reveal the potential for operational costs in the event of a sovereignty challenge. Even when control is maintained or ultimately recovered, the impact of responding can demand considerable time, resources and coordination–potentially limiting an enterprise’s freedom to act.

Having safeguards in place does not mean enterprises are equipped to demonstrate that those safeguards work. Supporting evidence is not always organized, kept current or readily accessible when needed. Reconstructing that evidence can absorb time and resources precisely when the business is trying to resolve the underlying challenge and maintain operations.

The business problem is not just whether enterprises can retain control when challenged, but whether they can prove it quickly and credibly without creating unnecessary operational friction.

[3] ‘Material disruption’ was not separately defined in the survey and reflects respondents’ own interpretation. The 30% figure refers to the overall outcome of the sovereignty challenge, including disruption associated with both retaining control and providing evidence of that control. The survey did not separately quantify the contribution of each.



Chapter 2

The IBM Digital Sovereignty Index

Diagnosing where proof of sovereignty is weak or strong–and benchmarking enterprise maturity.

Chapter 1 established the gap between retaining control and demonstrating that control fully and credibly when challenged, which can cost the enterprise both time and freedom of action.

The IBM Digital Sovereignty Index was developed to assess how far enterprises have progressed in closing this gap.

It measures the strength of evidence that enterprises can retain and demonstrate control across their critical digital estate–including whether they can establish who was accountable, demonstrate that controls worked, explain decisions and show how they responded when challenged.

The Index provides a benchmark of enterprise maturity, identifying where evidence of sovereign control is strongest or weakest and how responding enterprises compare. It is based on respondents' reported governance arrangements and supporting evidence, rather than an independent audit of participating organizations.

What we measured

Digital sovereignty extends beyond where data is stored. It cuts across the critical technology, AI, data and operations an enterprise depends on, and its ability to retain control when circumstances change.

The Index therefore assesses evidence of sovereign control across four enterprise pillars: **AI, Technology, Operations and Data.**

In reality, a critical business process can depend on all four simultaneously. For the purposes of the Index, these are measured separately to diagnose where evidence is stronger or weaker.

Across each pillar, the Index assesses the same six dimensions of sovereign control

Responsibility:
Can you prove who was accountable?

Trace:
Can you show exactly what happened?

Constraint:
Can you prove the controls were working?

Intervention:
Can you show how you responded and recovered?

Exit:
Can you prove you could change provider or recover operations if needed?

Legitimacy:
Can you explain and justify the decision under scrutiny?

Each enterprise surveyed received a **Digital Sovereignty Index score,** with scores placed into three maturity tiers: **Emerging, Establishing and Leading.**

What the average Index score reveals

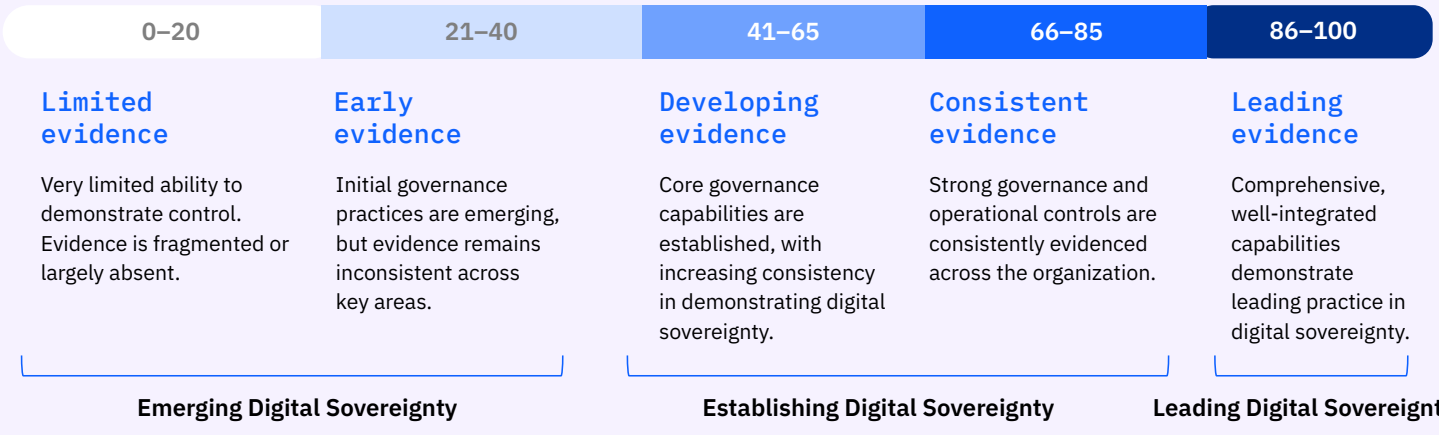
The global average Index score is **74/100**, placing the average enterprise in the 'Consistent Evidence' band–the upper evidence band within the broader 'Establishing' maturity tier, showing most surveyed enterprises have established foundations for demonstrating sovereign control.

However, the highest standard remains uncommon with only **26%** of surveyed enterprises reaching the Leading Digital Sovereignty tier (Index scores of 86–100)–where the Index measures more comprehensive, well-integrated evidence of sovereign control.

This tells us that the maturity challenge for most of these enterprises is not starting from zero. It is moving from evidence that is generally available to evidence that is comprehensive and demonstrably holds up under scrutiny. Progress is therefore less about adding governance, and more about having evidence that existing governance works.

Defining the Digital Sovereignty Index

FIGURE 4



Confidence runs ahead of evidence

Across the six dimensions of sovereign control, an average of **82% of surveyed senior decision-makers are very or extremely confident that their enterprise can provide the evidence required.**

Yet only **26% of surveyed enterprises reach the Index's Leading Digital Sovereignty tier**. Taken together, this reveals **a 56-point[4] overconfidence gap.**

The gap does not necessarily mean enterprises are wrong to believe evidence exists or can eventually be produced. But the Index applies a higher standard: whether evidence is sufficiently comprehensive and credible to demonstrate control when required. As we have seen–for most challenges, formal evidence will be required.

Regulator interviews describe a related risk: weaknesses in evidence and accountability can remain hidden until an incident, audit or other request demands proof.

The operational consequences can be severe. Critical business activity or technology updates may be delayed, senior executives may be drawn into the response, and the enterprise's freedom to act can be constrained at precisely the moment it needs to respond or change course.

> "The risk of overconfidence definitely exists. Many organizations tend to think they have 'control' because they have policies and contracts in place, but when it comes to audits or incidents, they may find that they don't have the objective evidence to back it up.
>
> The gap is invisible during normal times and only becomes apparent in situations where 'proof from the outside' is required, such as external audits, major incidents, information disclosure requests, and lawsuits.
>
> If evidence is insufficient at that time, accountability cannot be fulfilled, regardless of whether control was in place or not."
>
> **AI Governance Advisor**
> Japan

Leading evidence vs confidence

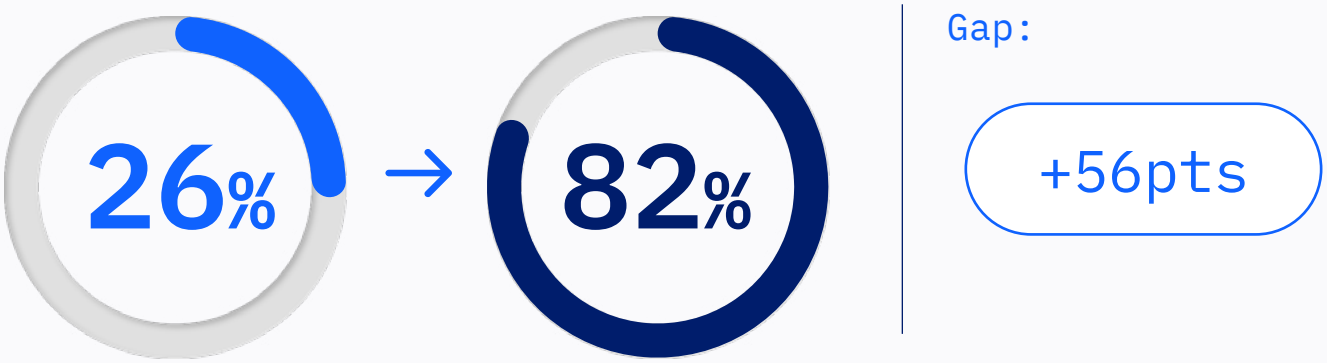
FIGURE 5

Leading evidence

% of organization scoring a digital sovereignty index of 86-100

Confidence

(Very or extremely)
Average confidence in providing evidence across dimensions



[4] The 82% figure is the average proportion of senior decision-makers who are very or extremely confident across the six evidence dimensions; 26% is the proportion of enterprises in the Leading Digital Sovereignty tier. The comparison therefore contrasts reported confidence with highest-tier evidence maturity, rather than two identical measures.

Barriers to proof span systems, providers and accountability

Respondents cited manual evidence collection (56%), fragmented evidence across teams and systems (53%), dependence on third parties for records and information (53%) and legacy systems or inconsistent standards (53%) as the biggest hurdles. Untested controls, recovery or Exit arrangements were also cited as a barrier by 50% of respondents.

Fragmented evidence can force teams to reconstruct the record after the fact, adding time and operational effort when scrutiny is highest. Unclear accountability can create gaps in escalation and make it harder to provide a coherent account of what happened. Untested exit arrangements can leave an enterprise uncertain whether it can actually change providers or maintain service continuity. Legacy and proprietary systems can make evidence harder to reconstruct or extract, while third-party dependencies can delay access to the information urgently needed to establish what happened.

> “Depending on the technology, switching provider can take anywhere from three to six months. And all of this, of course, comes at a cost–and quite a significant one. So even if there were a compliance issue, you wouldn’t necessarily be able to leave the supplier immediately.”
>
> **Public sector technology leader**
> France

It is worth noting that no single barrier was cited by respondents much more than any other, as this reveals how friction is distributed fairly equally across evidence, systems, providers and accountability, rather than being concentrated in a single weakness.



> “If it takes two or three months, or longer–and a team of 40 people to find and reconstruct evidence to respond to a real audit, perhaps from a central bank–then in my view, you’re not on top of it. You’re not in control.”
>
> **Dennis Lauwers, VP and CTO**
> Sovereign Technologies and Hybrid Automation, EMEA, IBM

Responsibility is the greatest blind spot

Responsibility–the ability to prove who is accountable for decisions and outcomes–has the **largest confidence-evidence gap** across all four enterprise pillars measured by the Index.

This means surveyed enterprises are more confident in their ability to prove accountability than the findings support. It points to a gap between knowing who is responsible and being able to prove who had authority.

When a critical service depends on an external provider, such as a cloud or AI provider, the enterprise still needs to be able to demonstrate *who* owns the business outcome, who has authority to act and *how* responsibilities are divided between the enterprise and its suppliers.

> "If a company doesn't put sovereignty as a business requirement, they will make specific business decisions–for example use the native features from a provider as fast and efficiently as possible. Then the day they have a problem, they could find that they can't make a switch, can't afford to make it, or can't explain it clearly. That early decision impacts future choices in ways they can't always anticipate–mitigating that in the technology and in the operations is the key to designing for sovereignty."
>
> **Giovanni D'Aniello**
> Group Chief Information Officer, AXA

Prepared to Exit is not the same as proven Exit

Another important distinction revolves around dependency and exit strategy. Having a documented exit plan is not the same as proving that a critical provider, model or system can be replaced while maintaining business continuity.

Dependence on external providers is not inherently incompatible with digital sovereignty. The risk arises when an enterprise has limited ability to change course if a critical provider becomes unavailable, its terms change or its services no longer meet business or regulatory requirements.

As with Responsibility, Exit is another dimension where overall confidence in enterprises' ability to provide evidence runs ahead of the specific evidence measured by the Index, across all four pillars. During their most testing sovereignty challenge, only **33%** of enterprises reported being able to demonstrate Exit fully and credibly, without significant follow-up, while **50%** identified untested controls, recovery or Exit arrangements as a barrier.

Proving Exit requires more than identifying an alternative supplier. Enterprises need to establish whether critical data, workloads and controls can actually be transferred, whether responsibilities are clear and whether operations can continue during the transition.



> "Even if migration rights are written in the contract, it is meaningless if the migration cannot actually be done. Therefore, verified portability–that is, migration tests using actual data and confirmation of the possibility of exporting in standard formats–is critically important."
>
> **AI Governance Advisor**
> Japan

AI is where pressure is reported highest and where evidence of control appears weakest

The research suggests AI is raising the bar for what sovereignty requires, as the technology becomes more deeply integrated throughout business operations and agentic systems increasingly act on behalf of the enterprise.

> "As AI becomes embedded across the enterprise, thinking through the many layers of sovereignty is a matter of business continuity in an age where technology is essential to run an enterprise and continue building trust."
>
> **Emmanuel Frenehard, Chief Digital Officer**
> Sanofi

AI-related issues were the most commonly experienced individual sovereignty challenge, cited by **44%** of respondents. At the same time, AI is the lowest-scoring Index pillar at **68.7**, showing proof of control is least mature in this area. While the other three pillars score higher, all four remain within the Index's Consistent Evidence band rather than reaching the Leading standard.

AI issues came ahead of other situations respondents reported experiencing over the same three-year period, including formal audit or regulatory events (38%), significant provider changes (35%) and data-access or transfer issues (33%). Government restrictions–such as export controls, sanctions or foreign-jurisdiction issues affecting access to technology, AI models, data, providers or operations–were reported by 30% of respondents.

Perspectives from customer leaders highlighted how, as AI systems take on more decisions and actions, the sovereignty questions become more demanding: where do these systems operate, which decisions do they influence, who remains accountable and who can intervene if a service fails?

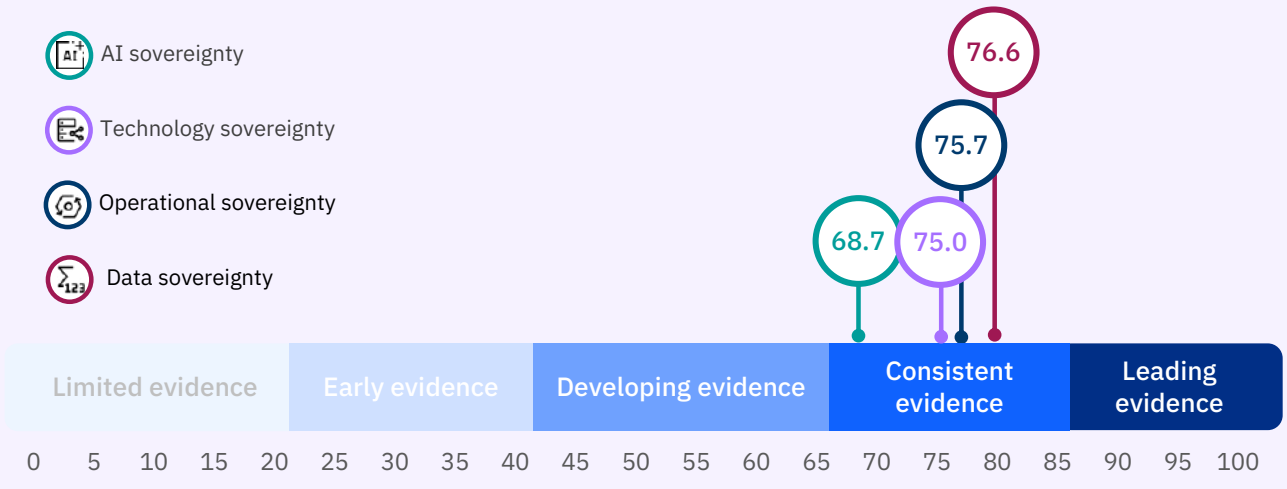
The literature review and qualitative interviews suggest that established governance disciplines are being stretched as enterprises apply existing controls around data, technology and operations to rapidly evolving AI systems and the new dependencies they create.

AI therefore needs to be governed as part of the wider control environment, rather than treated as a separate technology challenge.

> "Consider an enterprise that loses access to a critical AI model. If the cause is a network failure, restoring connectivity or switching clouds may resolve a resilience issue. If an external authority or provider decision restricts access to the model, the enterprise may face a sovereignty challenge. Simply switching clouds may not restore access. Instead, it may need an alternative model or provider, potentially with different performance or behavior."
>
> **Dennis Lauwers, VP and CTO**
> Sovereign Technologies and Hybrid Automation, EMEA, IBM

Index performance across Sovereignty pillars

FIGURE 6



Innovating with AI while protecting mission-critical performance

Finanz Informatik runs IT for Germany's savings banks, supporting 50 million customers and around half of the country's retail banking. Detlev Klage, Vice Chairman, describes its systems as "mission critical for the economy."

As it expands its use of AI, Finanz Informatik ensures a balance between innovation on the one hand and the stability, security, and regulatory requirements of core banking operations on the other. Its strategy, therefore, is to host data and applications–such as AI models–in its own data centers. It also preserves the freedom to choose between different AI models, including the ability to switch models as soon as better ones become available, as well as to keep costs predictable and respond flexibly to business needs.

Those requirements influence how AI is deployed in practice. One example is instant payments, where transactions can complete within ten seconds–creating a correspondingly short window in which to identify potential fraud. Finanz Informatik first introduced AI-based risk assessment to classify transactions, before moving to real-time verification within that ten-second window.

The performance and resilience requirements led Finanz Informatik to run the capability on its mainframe, avoiding a platform change.

What Leading enterprises do differently

The value of the Index as a maturity benchmark is not simply that it separates enterprises into tiers. It also allows businesses to compare how enterprises at different maturity levels operate, the friction they encounter and what happens when sovereignty is tested.

Across those comparisons, a consistent pattern emerges.

Leading enterprises surveyed test more regularly, report fewer barriers to producing proof, demonstrate stronger evidence under scrutiny and are more likely to resolve their most testing sovereignty challenge without material disruption.

Leading enterprises make testing routine and report fewer barriers to proof

The Index shows how testing frequency rises sharply with maturity among surveyed enterprises: just **9%** of Emerging enterprises test continuously or through regular governance and assurance, compared with **29%** of Establishing enterprises and nearly **two-thirds (63%)** of Leading enterprises.

Leading enterprises surveyed also report fewer barriers when they need to provide evidence or demonstrate control, including legacy systems, legal restrictions, unclear ownership and incomplete evidence.

"We believe AI will be essential to future resilience, but that means more than adopting individual use cases. It will come from a comprehensive strategy. Our focus is always on our customers, which means having the flexibility to deploy the right models across a complex, multi-tenant environment while maintaining the security, reliability and quality they expect.

Digital sovereignty is of paramount importance to FI and serves as the foundation for the highest level of security as well as for the stable and efficient operation of the savings banks' infrastructure."

Detlev Klage, Vice Chairman
Finanz Informatik



Frequency of organizations testing its ability to demonstrate digital sovereignty

FIGURE 7

% of organizations continuously or as part of regular governance and assurance processes



Continuous testing increases with Digital Sovereignty maturity

Stronger evidence maturity is associated with better outcomes

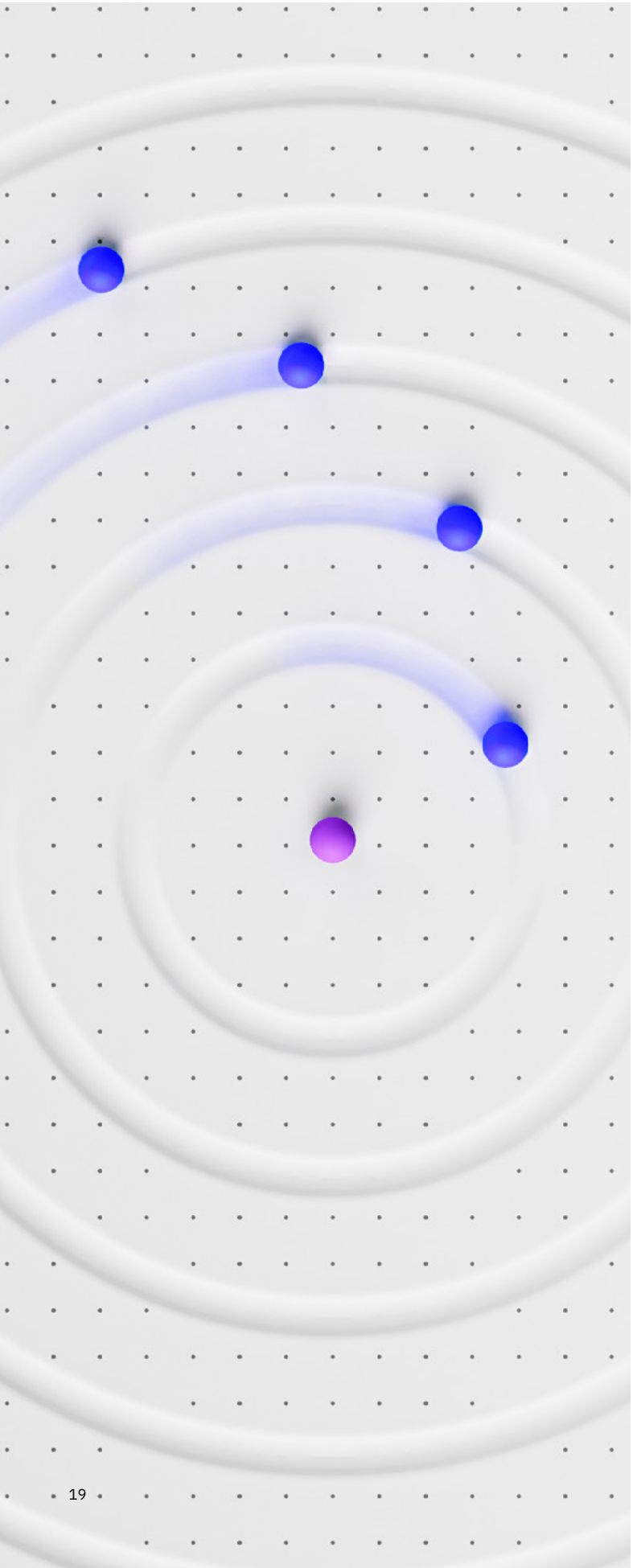
Across all six dimensions of sovereign control, Leading enterprises surveyed were more likely than Establishing enterprises to demonstrate control fully and credibly, without significant follow-up, during their most testing sovereignty challenge–an advantage of **8 to 19 percentage points**, depending on the dimension.

For business leaders, this can matter because questions about who was accountable, what happened, whether controls worked and what options remain available may need to be answered while the enterprise is still responding to the underlying challenge.

The difference also appears in the overall outcome. **52% of Leading enterprises resolved their most testing sovereignty challenge without material disruption, compared with 22% of Establishing enterprises–making Leading enterprises more than twice as likely to report this outcome.**

While the research does not establish that higher evidence maturity caused the better outcome, it does show that enterprises with stronger evidence of sovereign control are also more likely to report resolving sovereignty challenges without material disruption.

The Index shows where evidence maturity falls short and what distinguishes enterprises that perform better under scrutiny. The next challenge is translating those differences into an operating model that keeps capabilities tested and evidence ready as systems, providers and business requirements change.



Chapter 3

IBM Perspective: A new operating model

Proof must be embedded in normal operations, with evidence kept current, accessible, and ready to withstand scrutiny.

Customer perspectives highlighted the challenge of keeping evidence current as systems and operating environments change. Evidence has a shelf life because AI models, business processes, data flows and technology components are continuously changing. Information that was accurate when captured can quickly stop reflecting the enterprise's current operating state.

Building on the Index findings and qualitative interviews, IBM recommends a shift from periodic proof toward an operating model of ongoing evidence readiness. Controls, evidence and accountability should be maintained through normal operations in order to remain observable, testable and provable.

The approach will vary by enterprise and event, but the aim is consistent: evidence that keeps pace as systems, providers and decisions change.

> "Digital Sovereignty is tested when conditions change, not when everything is running normally. Organisations need to be able to demonstrate control through enforceable security, auditable compliance and clear governance, with the ability to intervene, recover or change providers when risk increases without disrupting the business. The goal is not simply to satisfy policy requirements, but to build resilience into the way technology is operated every day"

Graeme Smith, Chief Technology Officer
Celerity UK

Proof depends on ongoing visibility and evidence of control

Enterprises should know what is changing, who or what is acting, which controls apply and where the supporting evidence sits *before* anything goes wrong.

This requires visibility across critical systems, controls and dependencies. For example, monitoring AI models and agents, together with retaining relevant operational records, can help enterprises establish what those systems did, which data they used and what controls governed their actions.

Visibility also needs to extend beyond individual technologies. Enterprises must understand how critical systems, data, AI models and external providers interact, and whether the controls and evidence needed to demonstrate sovereignty remain accessible across them.

Customer perspectives highlighted how logs, telemetry, backups and other operational records can sit across multiple systems or with external providers, outside the main control environment. This can make it harder to assemble a complete account when something goes wrong.

If those records are only discovered after the event, evidence collection once again becomes reconstruction.

> “The problem is not dependency itself, but dependencies you do not fully understand. Start by mapping your critical services, data and platforms, understand the dependencies behind them, and ask what happens if one becomes unavailable. Sovereignty isn’t about eliminating dependencies. It’s about consciously choosing and managing them.”
>
> **Fredrik Sidmar, CEO**
> Telia Cygate

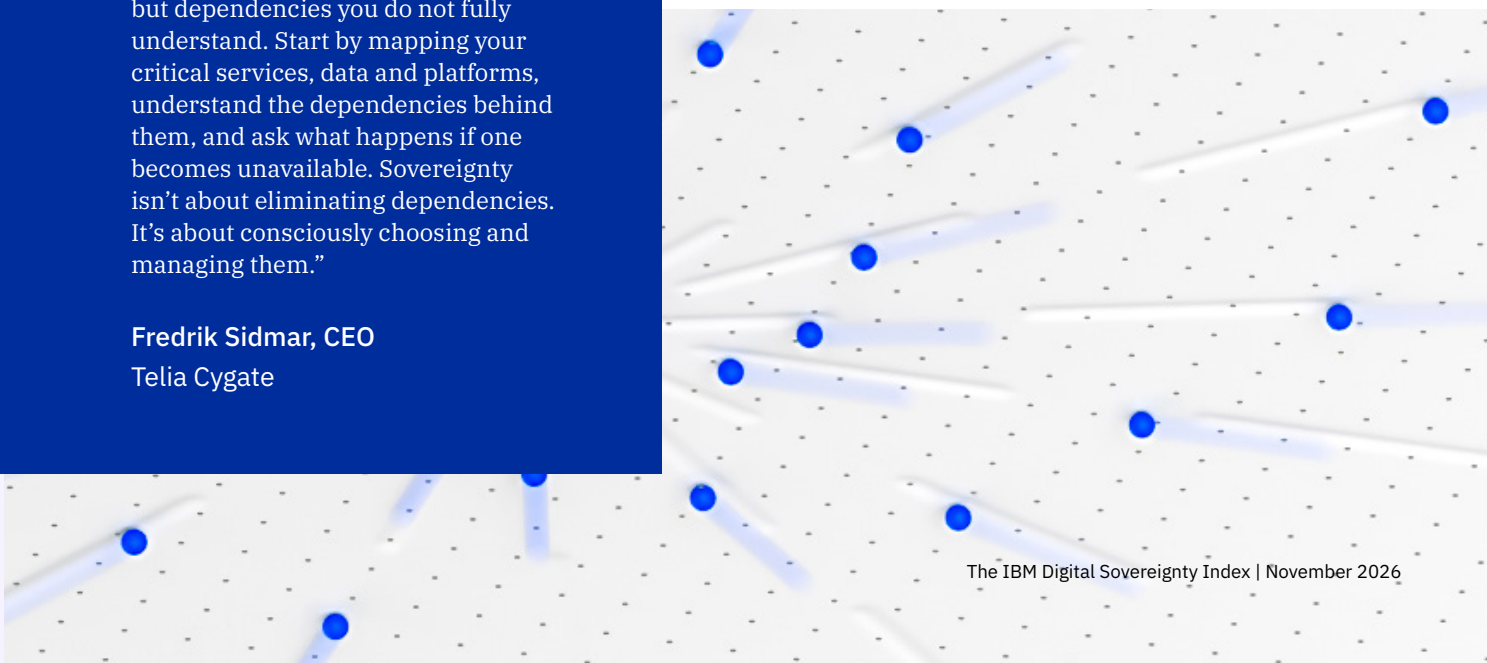
Test before you‘re tested

Regular testing is another critical element of IBM‘s proposed operating model.

Having ‘more evidence’ does not automatically mean stronger proof. Policymaker and regulator interviews emphasized the importance of demonstrating that sovereignty capabilities work in practice. This could mean testing whether an AI service can be stopped or overridden, whether events and decisions can be reconstructed from available records, or whether a critical system can be recovered or replaced while maintaining control.

Policymaker and regulator interviews also highlighted Exit as a key dimension where there is a need to *exercise* these capabilities rather than relying solely on arrangements on paper. Contractual migration rights or exit agreements are not enough if migration cannot actually be performed. Migration and failover tests, for example, were cited as providing stronger evidence than a documented right alone, because they test the capability itself. This indicates why maintaining a regularly ‘provable state’ involves verification and simulated exercises rather than merely self-reporting untested processes.

> “The mere existence of an agreement is meaningless unless drills verify that it can be effectively activated.”
>
> **Government regulator**
> Japan



Sovereignty as an ongoing discipline

Almost every enterprise surveyed appears to have made changes after being tested but only a minority test continuously before the next challenge arrives. Among surveyed enterprises that experienced a sovereignty challenge, **99% made improvements afterwards**.

That shows how effectively a real event can expose weaknesses and trigger change, but the stronger operating model is to build those lessons into day-to-day governance and assurance *before* the next test exposes those weaknesses.

The research shows that many surveyed enterprises are already moving in this direction: **one in three[5] test their ability to demonstrate sovereignty continuously or as part of regular governance and assurance processes.**

That is the shift from reactive learning to continuous readiness. Testing on this basis can help keep weaknesses visible and give enterprises repeated opportunities to strengthen controls and the evidence around them.

An enterprise can test continuously, but if evidence from those tests is not captured, learned from and kept accessible, it may still find itself reconstructing proof when a challenge arrives.

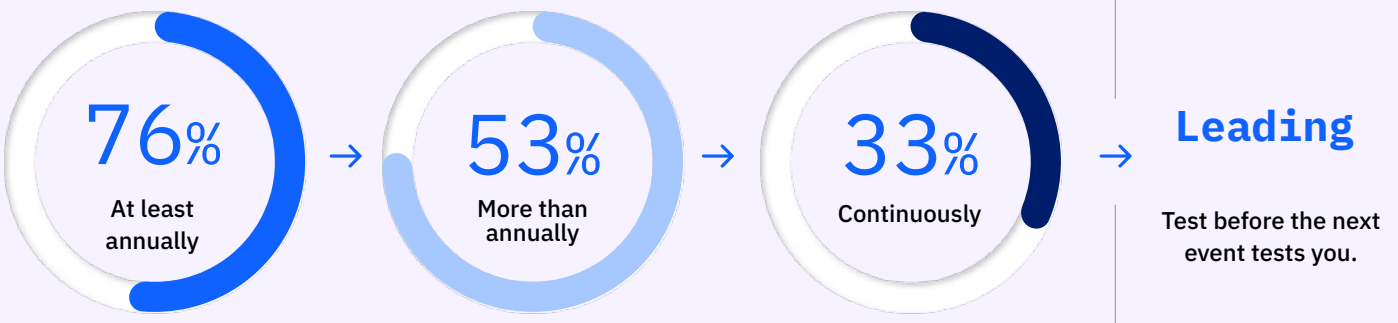
From capability in place to capability proven

The Index's higher evidence standards emphasize capabilities that have been tested, validated or demonstrated under scrutiny. The corresponding shift for enterprise operating models is from 'we have a plan' to 'we have exercised it and can show the result.'

Progress therefore depends on moving beyond established governance capabilities and controls to demonstrating that they have been tested and can withstand scrutiny.

How often organizations test their ability to demonstrate sovereignty

FIGURE 8



Test their ability to demonstrate sovereignty at least annually

Test more than once a year

Test continuously or as part of regular governance and assurance processes

63% of Leading Evidence organizations test continuously

99% made improvements after their most testing sovereignty event.

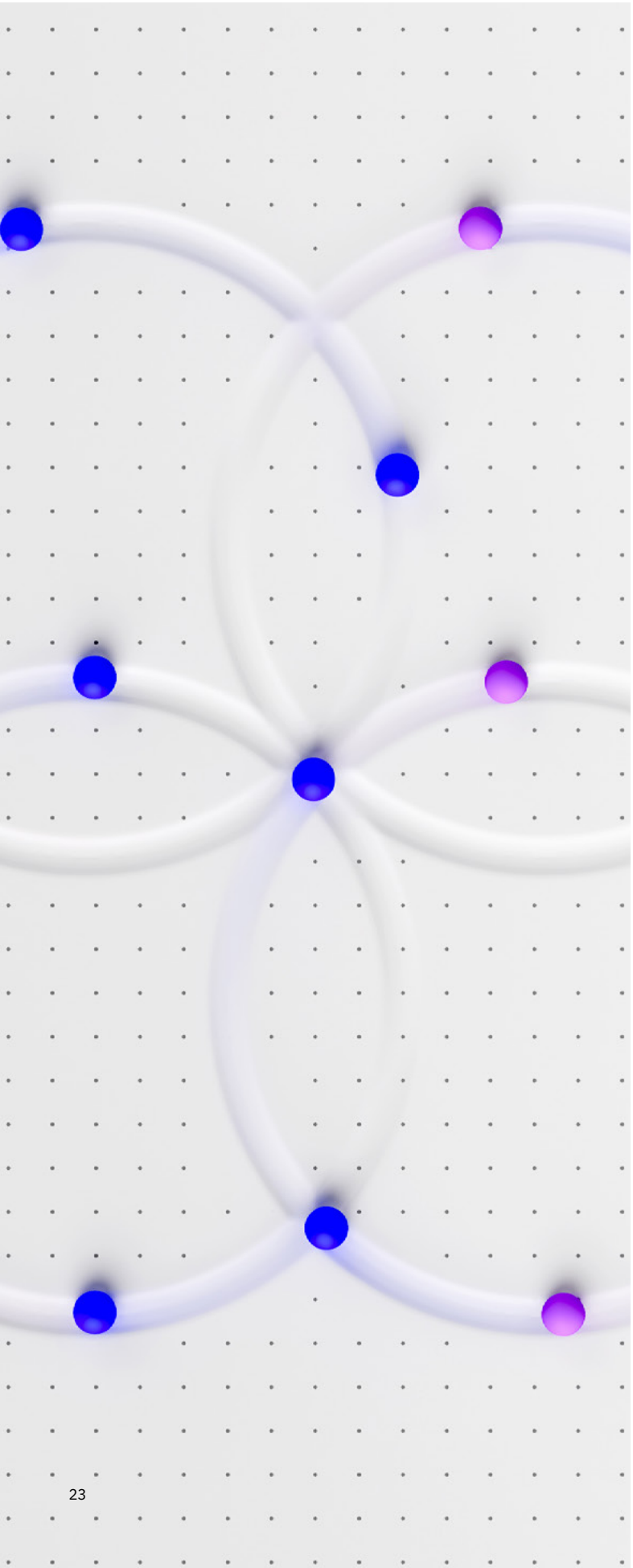
[5] The survey measured how often enterprises test their ability to demonstrate digital sovereignty and produce supporting evidence under scrutiny. The one in three (33%) finding refers to testing frequency; it does not establish that evidence is collected continuously.

FIGURE 9

Capability in place to capability proven

	FROM Capability in place	TO Capability proven
	**Responsibility** Accountability clearly assigned	Ownership proven under scrutiny
	**Trace** Detailed records retained	Complete audit trail
	**Constraint** Controls consistently applied	Controls routinely tested and independently reviewed
	**Intervention** Response procedures embedded	Readiness exercised and improved
	**Exit** Exit arrangements operationally ready	Exit successfully tested or used
	**Legitimacy** Governance and assurance in place	Assurance validated under scrutiny

One intended benefit of this operating model is to shorten the path from being challenged to producing credible proof. If evidence is already captured and accessible, the enterprise is in a stronger position to establish what happened and exercise its options while the business keeps moving.



Chapter 4

The leadership imperative

Digital sovereignty is not just a compliance or technology issue; it affects resilience, freedom of action and an enterprise's license to operate.

Enterprises running critical services need board-level oversight and clear executive accountability for digital sovereignty.

> "Digital Sovereignty is now a board-level conversation. As organizations accelerate the adoption of AI, they must ensure they retain control, authority, and accountability across their critical digital ecosystem. Sovereignty is grounded on a granular and consistent approach, following strong design principles. It requires having the right technology controls in place, but is only demonstrated by continuously proving resilience, compliance, and operational control in a fast evolving market."
>
> **Michael Nimhauser**
> **Global Head of Sovereignty**
> Atos

Technology, Risk and Compliance teams may implement many of the controls. But deciding which services cannot be allowed to stop, which dependencies the enterprise is prepared to accept and where to invest in resilience and proof are executive decisions.

What the highest evidence standard looks like

The Index's highest evidence standard is expressed differently across each of the six dimensions. Not every Leading enterprise will reach this level in every dimension, but together they show what 'capability proven' looks like in practice across AI, Technology, Operations and Data.



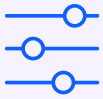
Responsibility

Accountability has been demonstrated under scrutiny–for example through audit, regulatory review, assurance or operational testing.



Trace

A complete audit trail exists–appropriate to the domain, such as model inputs and outputs, data lineage, infrastructure logs, approvals or incident records.



Constraint

Controls are routinely tested and independently reviewed[6].



Intervention

Response or intervention procedures are tested and improved using exercises or lessons learned.



Exit

Migration, switching, recovery or other exit arrangements have been successfully tested or used.



Legitimacy

Governance and assurance have been independently validated or successfully demonstrated under scrutiny.

[6] Independent review or validation refers to assessment by a function or party sufficiently independent of those responsible for operating the control. This may include internal audit, independent assurance teams or external reviewers, depending on the context. It does not necessarily require regulatory review.

Five leadership priorities

Drawing on the Index findings and qualitative interviews, IBM recommends five leadership priorities for enterprises to focus on.

01

Start with what cannot stop

Start with a small number of critical business processes and map the systems, data, AI models and providers they depend on. Prioritize investment where losing control would most threaten continuity, accountability or strategic choice.

Questions to ask include:

- What process cannot be allowed to stop?
- Which data, systems, models and providers does it depend on?
- Who actually controls those dependencies?
- What would we need to prove if this process were challenged tomorrow?

> “On a digital sovereignty strategy, start by mapping your most critical business processes to the technology that supports them. Once you understand where you have concentrated dependencies, develop and regularly test reversibility strategies. It is extra work, but it is worth doing.”
>
> **Giovanni D’Aniello, Group Chief Information Officer,** AXA

02

Make accountability end-to-end

Assign clear executive accountability for each critical process, including where delivery depends on external providers or AI systems.

Establish who owns the business outcome, who has authority to intervene or activate alternative arrangements when a critical dependency becomes unavailable or untrusted, and how decision rights are divided between internal teams and suppliers.

03

Make evidence readily available

Make evidence availability an investment priority. Identify what proof must currently be assembled manually, where it sits, who controls it and which records depend on suppliers.

Invest in integrating and automating evidence collection where appropriate. Work with critical providers to make relevant records accessible during normal operations, rather than relying solely on requests when scrutiny arrives.

04

Test intervention and exit–before you’re tested

Make intervention and portability part of supplier and architecture decisions. For the most critical dependencies, require teams to demonstrate that they can pause, recover, replace or migrate services while maintaining control and continuity–and establish when those capabilities were last tested.

For the most critical dependencies, ask:

- Can we intervene?
- Can we pause or override?
- Can we recover?
- Can we replace the provider or model?
- Can we migrate while preserving data, controls and continuity?
- When did we last prove it?

05

Make proof of sovereignty a continuous management discipline

Make the ability to demonstrate sovereign control a standing item in executive technology, risk and operational reviews.

Leaders should know which critical capabilities have been tested, whether supporting evidence is current, which weaknesses remain unresolved and who is accountable for addressing them as systems and dependencies evolve.

Capabilities that support the leadership agenda

These leadership decisions also need to shape technology architecture. Sovereignty by design emphasizes embedding governance and visibility across the technology environment, while using open, portable architectures to help reduce excessive dependencies and preserve freedom of choice.

This means maintaining the ability to move workloads, replace models or change providers without losing control. The technologies that support these capabilities will depend on the critical processes and dependencies the enterprise needs to protect, but can include:

Integrated evidence collection:
Keeps logs, approvals, model records, lineage and other evidence current and accessible.

Automated orchestration:
Coordinates repeatable workflows and reduces manual intervention.

Integrated control and visibility:
Makes governance, access, dependencies and operational status more observable.

Governed AI services:
Provides clearer policy, access, oversight and evidence around models and agents.

Open and hybrid architectures:
Support portability and deployment choice, reducing the risk of lock-in to individual platforms or providers.

> "It's no longer only about protecting what matters. Nations see digital sovereignty as a vehicle for better citizen services and, over time, greater innovation and economic growth. With technology advancing, speed becomes just as important as control. At AMD, we believe proven, open technologies and flexible solutions make both possible, enabling innovation without sacrificing resilience, independence and choice."

Philip Guido, EVP & Chief Commercial Officer
AMD

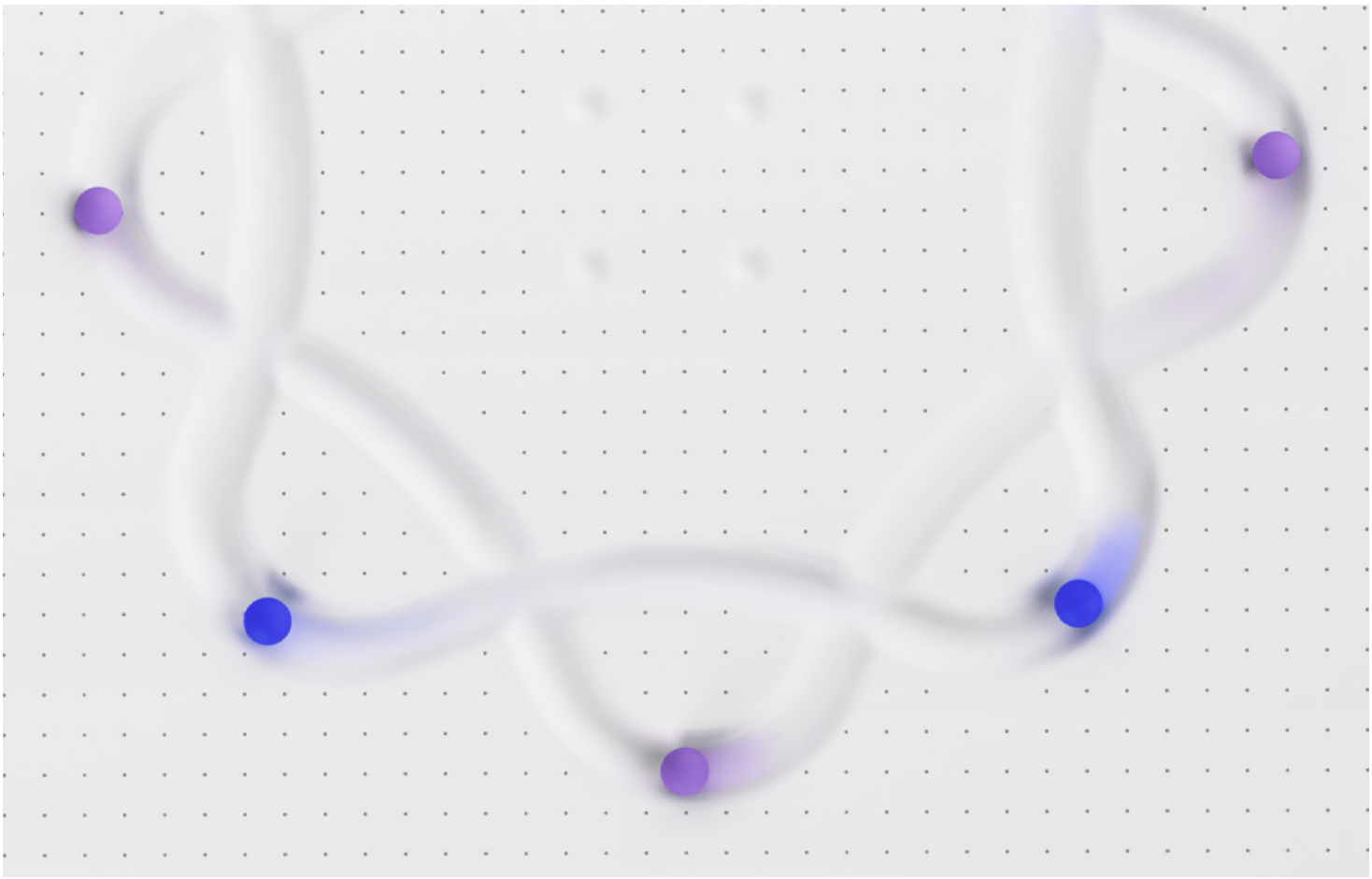
> "European organizations–from public authorities to critical infrastructure providers–have been unequivocal with us. They need the most advanced AI-driven security capabilities available, and they need verifiable sovereignty controls over their data. What we have learned, and what drives our approach, is that these two requirements are not in tension. That is the standard we are holding ourselves to."

Helmut Reisinger, CEO
Palo Alto Networks, EMEA

Enterprises are planning for control. Leaders must plan for proof.

Control without proof creates operational exposure. Leaders must therefore make the ability to demonstrate control an explicit requirement in decisions about critical services, suppliers, architecture and investment.

The next sovereignty challenge may be impossible to predict. But an enterprise should not have to discover what it can prove at the moment it needs to act. The objective is to keep operating, account for critical decisions and retain the freedom to change course–with evidence that holds up under scrutiny.



Further information and resources

Get in touch

Book a meeting to discuss your Digital Sovereignty challenges

Take the IBM Digital Sovereignty Assessment for your organization

Learn more

Learn more about IBM Digital Sovereignty Solutions

Read 'The Calculus of AI Sovereignty' from the IBM Institute for Business Value

Subscribe to IBM's monthly IdeaWatch newsletter

Methodology

The Digital Sovereignty Index is based on a multi-stage global research program combining a literature review, qualitative interviews and a quantitative survey. Together, these three stages were used to establish the conceptual foundations of digital sovereignty, develop and validate the Digital Sovereignty Index, and benchmark organizations' ability to demonstrate retained control across Data, Technology, Operations and AI.

01
Literature review

A review of **27 sources** was conducted, spanning legislation, standards and governance frameworks, academic research, thought leadership and the IBM Digital Sovereignty Readiness Assessment.

The review covered the four core domains of digital sovereignty–**Data, Technology, Operations and AI**–and examined relevant sources from the US, UK, Germany, the EU, India, Japan and Saudi Arabia.

02
Qualitative research

The research included **25 x 45-minute virtual in-depth interviews** with regulators, policymakers, public-sector officials and policy experts across seven markets: the United States (5), United Kingdom (3), Germany (2), India (4), Japan (4), France (3) and Saudi Arabia (4).

Participants brought perspectives spanning technology, AI, data governance, cloud, cybersecurity and related policy areas. These interviews were complemented by perspectives from **17 senior customer leaders across five countries**–Spain (9), United States (5), United Kingdom (1), Germany (1) and Belgium (1)–representing senior roles across technology, cloud, AI, data, security, risk, compliance and operations.

03
Quantitative research

A **20-minute online survey of 2,003 senior decision-makers** was conducted across seven markets: the United States (500), United Kingdom (250), Germany (251), India (251), Japan (251), France (250) and Saudi Arabia (250).

Respondents held responsibility for areas including data, AI, technology, operations, governance, risk and compliance within large enterprises. The survey provided the quantitative evidence used to validate the framework and benchmark organizations through the Digital Sovereignty Index.

The Digital Sovereignty Index

The Index combines evidence across **Data, Technology, Operations and AI** into an overall Digital Sovereignty score reflecting an organization's ability to demonstrate retained control. It enables organizations to benchmark their position, identify strengths and pinpoint areas where stronger evidence may be required.

The Index is based on survey respondents' reported governance arrangements and supporting evidence. Participating organizations were not independently audited as part of the research.

Throughout this report, **Emerging, Establishing and Leading** refer to the three Digital Sovereignty Index maturity tiers. The Index measures demonstrated evidence of sovereign control–while digital sovereignty itself is the broader organizational challenge.

Sample note: Survey participants worked at enterprises with 1,000+ employees in the US, 100+ in Saudi Arabia and 500+ employees in all other markets.

