August 2026
White Paper
Sponsored by Commvault

Securing the Future: Data Protection and AI Governance in Financial Services with Commvault and AWS

Christopher Lee Marshall
Vice President,
Data, Analytics, AI, Sustainability,
and Industry Research, IDC

Jerry Silva
Program Vice President,
Financial Insights, IDC

Table of contents

Click any title to navigate directly to that page.

IDC opinion 3

Situation overview 5

Introduction 5

Survey insights: The state of data protection in financial services 6

AI governance and emerging security challenges 7

Regulatory alignment and data sovereignty 9

Economic considerations of data risk management 10

The Commvault + AWS advantage 12

Challenges and opportunities 14

Strategic recommendations 16

Conclusion 18

About the IDC analysts 20

IDC opinion

IDC's *Custom Survey for Commvault,* October 2025 (n = 250 respondents from banking, insurance, and capital markets in the United States, the United Kingdom, Australia, and India) finds that data protection and AI governance have moved from back-office concerns to board-level priorities in financial services.

Firms are no longer simply asking whether they can back up and restore workloads. They are asking whether current architectures can support immutable protection, verifiable recovery, regulatory scrutiny, and AI innovation on a cloud foundation. The fact that all respondents use AWS in production, and that more than half of datacenter real estate is now cloud based, shows that the center of gravity for resilience has shifted. Most institutions now operate hybrid estates in which on-premises platforms have long sat alongside cloud-native workloads. In this context, the Commvault and AWS partnership is strategically important because it directly addresses the need for unified control over data that is increasingly distributed, highly regulated, and deeply intertwined with AI initiatives.

IDC data suggests that many institutions have made significant progress on core resilience capabilities yet still face structural gaps. High adoption of immutability, with more than 60% of critical datasets protected in write once, read many (WORM) formats, and the ability of roughly two-thirds of firms to restore workloads to alternate AWS regions indicates that foundational controls are in place for many. At the same time, the need for two-thirds of organizations to re-architect backup and replication to meet data localization requirements underscores how fragile earlier designs can be when regulations tighten. Institutions that treat data protection as an integral part of cloud and data architecture, rather than an afterthought, will be better positioned to absorb future waves of regulatory and business change.

AI adoption sharpens this tension. Nearly half of respondents are already using AI in full production with sensitive data, and most have introduced controls such as governed retrieval, prompt logging, and denial of default training on regulated data. These are positive signals that financial institutions understand the need for explicit AI guardrails. However, only about half feel fully prepared to demonstrate AI governance controls to regulators. IDC interprets this gap as a sign that controls are often implemented in silos, tied to specific tools or pilots rather than anchored in a consistent data protection and governance framework. As AI workloads expand across business lines, firms will need platforms that can extend immutability, lineage, access control, and recovery into vector stores and model artifacts with the same rigor applied to traditional datasets.

The economics of resilience are also coming into better focus. The survey indicates that data protection now consumes nearly half of IT and cloud budgets on average, with more than 90% of firms increasing spending over the past year. Ransomware insurance is widespread, yet coverage alone does not reduce operational or reputational risk if recovery capabilities are fragmented or untested. IDC expects financial institutions to place greater emphasis on rationalizing overlapping tools; consolidating onto platforms that can cover on-premises, cloud, and AI workloads; and calibrating expenditure to measurable resilience outcomes, such as recovery time, recovery point objectives, and compliance readiness. In this environment, partnerships such as Commvault and AWS, which combine cloud-scale capabilities with proven data protection and cyber-recovery vault capabilities, will be evaluated not just on feature breadth but also on their ability to reduce complexity and the total cost of resilience.

Looking ahead, IDC sees unified data protection and cyber-resiliency foundations as critical enablers of modernization and an emerging prerequisite for AI governance readiness in financial services. Institutions that prioritize proven immutability, isolated recovery copies (including vaulting patterns), automated discovery of sensitive data, and reliable cross-region recovery will be better prepared for both regulatory scrutiny and unexpected disruption. As AI use expands, firms will also need to apply these controls to AI data foundations (such as training datasets, feature stores, vector databases, and model artifacts) so that recovery and audit evidence extends beyond traditional datasets. Commvault and AWS together represent one path to this outcome, particularly for organizations that have standardized on AWS as their primary cloud and want integrated resilience across hybrid estates and cloud-native services. IDC expects buyers to increasingly favor solutions that combine strong regulatory alignment, measurable resilience outcomes, and practical support for emerging AI patterns without creating new tool silos.

Situation overview

Introduction

Data environments in financial services are becoming more complex and more fragmented.

Core systems still sit on premises, yet critical workloads now run across multiple clouds and regions, often as cloud-native services, with separate teams and tools managing each layer. Data moves continuously between production systems, analytics platforms, and AI pipelines. As a result, firms must protect and govern information that is not only high volume but also highly distributed and constantly in motion.

At the same time, regulatory expectations are tightening. Frameworks such as DORA in Europe, evolving SEC rules in the United States, and a growing range of data localization requirements are raising the bar for resilience, transparency, and control. Regulators expect firms to demonstrate that they can withstand disruption, recover quickly, and prove the integrity and location of their data. This is no longer a periodic compliance exercise. Instead, compliance is now a continuous capability that must be designed into data architecture from the start.

AI adoption adds another layer of complexity. Financial institutions are training and deploying AI models on datasets that include client information, trading records, and other sensitive content. These initiatives can unlock value, but they also introduce new attack surfaces and governance questions. Firms now need to extend long-standing practices in data protection, access control, and auditability into AI workloads. The institutions that succeed will be those that treat AI, cloud, and on-premises environments as a single, broad risk surface and build data protection and governance strategies that span all three.

Survey insights: The state of data protection in financial services

The survey findings highlight that data protection decisions sit close to the center of power within financial institutions. With 88% of respondents acting as primary decision-makers for data protection, the choices made about platforms, architectures, and operating models reflect a direct link between business risk and technology strategy. These are not peripheral stakeholders. They are senior leaders who must balance regulatory scrutiny, operational resilience, and cost discipline while supporting rapid digital and AI-driven transformation.

The results also confirm that cloud is now a core component of the production environment. Slightly more than half of datacenter real estate is now cloud based, and every respondent uses AWS in production for at least some workloads. This combination points to a hybrid reality. Legacy platforms and data stores remain on premises, often embedded in critical trading, risk, and core banking processes, while new, cloud-native applications and analytics environments are growing rapidly in AWS. Data protection strategies must therefore span both worlds. Tools and processes that focus on a single environment are increasingly misaligned with how firms operate in real life.

Immutability has become a standard expectation for critical data, not a niche feature. The finding that 60.6% of critical datasets are protected with WORM controls indicates that many institutions have internalized lessons from ransomware, insider threats, and accidental deletions. Immutable storage does not replace broader security programs. Still, it provides firms with a reliable last line of defense that supports both operational recovery and evidentiary requirements in the event of disputes or regulatory investigations. In practice, many institutions are also pairing immutability with additional resilience measures such as isolated or logically air-gapped recovery copies and geo-redundant storage so that recovery data is protected even if production environments are compromised. The remaining portion of critical data that is not yet

protected in this way represents a clear focus area, especially for workloads that underpin customer-facing services or risk calculations.

Restoration capabilities are equally important. The fact that 67.9% of respondents have successfully restored workloads to alternate regions, while still meeting agreed recovery time objectives (RTOs) and recovery point objectives (RPOs), suggests that resilience testing has moved beyond theory for many organizations. These firms have demonstrated they can leverage AWS' regional diversity to manage outages, cyber-incidents, and localized disruptions. However, this still leaves a minority that has not proven cross-region recovery in practice. For these institutions, the risk is not only downtime. It is also the inability to credibly demonstrate resilience to regulators, rating agencies, and counterparties that now ask more detailed questions about continuity plans.

Taken together, these survey insights describe a sector that has embraced hybrid and cloud-based operating models and has made progress on immutable protection and cross-region recovery. At the same time, they reveal uneven maturity. Some firms are already treating data protection as a core part of hybrid and cloud-native architecture, while others are still relying on fragmented tools, manual processes, and untested playbooks. This divergence sets the context for the rest of the findings, particularly as AI, regulation, and economic pressure converge.

AI governance and emerging security challenges

The survey confirms that AI has moved beyond proof of concept for many financial institutions. Nearly half of respondents are using AI in full production with sensitive data, which likely includes client profiles, transactional histories, communications records, and internal financial data. This shift increases the stakes. When AI systems touch sensitive information, failures in access control, model behavior, or recovery can cause direct customer harm, regulatory breaches, and reputational damage.

Controls around AI workloads are starting to crystallize. A majority of firms report using governed retrieval, with role-based or attribute-based access control to manage which data is exposed to which models and to which users. Prompt and response logging is also common, which helps create an audit trail for investigation, quality review, and compliance. In addition, over half of the respondents deny default training on regulated data, which is

an important measure to prevent inadvertent leakage of sensitive information into model parameters, where it becomes harder to manage.

These practices are encouraging, yet they are insufficient given the evolving operating environment. Many of the controls described are application level or pipeline specific. They often depend on the configuration of a particular orchestrator, gateway, or model hosting platform. Without a strong underlying data protection and governance foundation, AI control planes risk becoming a new layer of siloed policy. For example, an AI application might restrict access at the prompt level, while copies of the same data live in less controlled backup, test, or analytics environments. Attackers and auditors do not care which layer fails, only that the overall environment is either secure and compliant or it is not.

With 96% of respondents stating that resilience and recoverability are critical to AWS migration, AI workloads are being evaluated through the same lens as core systems.

The importance of resilience in this context is evident. With 96% of respondents stating that resilience and recoverability are critical to AWS migration, AI workloads are being evaluated through the same lens as core systems. Firms increasingly recognize that AI applications and their underlying data stores, including vector databases and feature stores, will become part of critical business services. They will therefore need clearly defined RTO and RPO targets, tested failover paths, and consistent recovery strategies. An AI-enabled customer service platform that cannot be restored after a cyber-incident introduces as much risk as a legacy payment system that fails during peak volume.

Yet only 49.6% of respondents feel fully prepared to demonstrate AI governance to regulators. This gap between technical controls and regulatory confidence is significant. It suggests that firms are still working through how to document AI decision flows, tie model behavior back to data lineage, and prove that data minimization and access

policies are enforced in practice. It also indicates that many institutions have not yet integrated AI governance into broader operational resilience frameworks. For vendors and partners, including Commvault and AWS, this is an opportunity to show how data protection, observability, and AI controls can be combined into a coherent story that stands up to regulatory review.

Regulatory alignment and data sovereignty

Regulation is clearly reshaping the way financial institutions think about data protection architecture. Nearly two-thirds of respondents believe that their immutability and audibility capabilities align with regulatory expectations. This is an important signal. It shows that controls such as immutable storage (including WORM where appropriate), isolation or vaulting patterns for recovery copies, geo-redundant backup and replication, comprehensive logging, and tamper-evident audit trails are becoming part of standard operating practices for critical workloads.

However, this confidence coexists with substantial architectural disruption driven by data localization and sovereignty requirements. Two-thirds of organizations have had to redesign backup and replication strategies to keep data within specific jurisdictions or to ensure that certain categories of data do not leave a prescribed region. These changes are rarely simple. They can affect where backups are stored, how replication is configured across AWS regions and availability zones, and how disaster recovery plans are structured. They may also require new segregation of duties and changes to vendor contracts.

The fact that 77% of respondents who re-architected for localization already have a cyber-recovery vault in full production is telling. It suggests that many institutions are pairing regulatory-driven changes with a broader shift toward more robust recovery capabilities. A dedicated cyber-recovery vault, properly designed, can help isolate clean copies of critical data, support faster restoration during cyber-incidents, and provide a trusted baseline for regulatory attestations. When combined with strong immutability and audibility, it can also help institutions prove that data has not been altered, deleted, or exfiltrated during an event.

Yet regulatory alignment remains a moving target. Frameworks such as DORA, evolving SEC and prudential guidelines, and local data sovereignty rules are still being interpreted and applied. Supervisors are asking more detailed questions about how firms classify critical functions, map dependencies, and ensure that the data needed to support those functions is protected and recoverable in all scenarios. In this environment, architectures that are hard coded to a specific regulatory interpretation are vulnerable to future change. Architectures that are modular, policy-driven, and capable of consistently

enforcing localization, immutability, and access control across hybrid and cloud-native environments are more likely to remain resilient as regulations evolve.

For Commvault and AWS, this landscape reinforces the importance of solutions that can operate at the intersection of technology and regulation. Financial institutions are not only looking for tools that can perform backup and recovery; they are looking for platforms that can help them enforce data residency policies, provide clear evidence of control effectiveness, and align recovery capabilities with regulatory definitions of critical services. The survey results suggest that many organizations have begun this journey, yet there is still room to strengthen the link between data protection design and regulatory strategy.

Economic considerations of data risk management

The economics of data protection in financial services are shifting from discretionary projects to structural investment. An average spend of 49% of IT and cloud budgets on data protection–related activities indicates that resilience, backup and recovery, security controls, and governance tooling are now major cost centers. This level of investment reflects both the growing threat landscape and the rising cost of non-compliance. It also raises questions about efficiency. When nearly half of technology budgets are tied up in protection and control, firms must ensure that every dollar contributes to measurable risk reduction.

An average spend of 49% of IT and cloud budgets on data protection–related activities indicates that resilience, backup and recovery, security controls, and governance tooling are now major cost centers.

The fact that more than 90% of respondents report increased data protection spending in the past 12 to 18 months underlines this point. Many institutions have responded to high-profile ransomware attacks, regulatory pressure, and internal risk reviews by adding new tools, hiring specialists, and upgrading infrastructure. While this may have been necessary to close immediate gaps, it can also lead to sprawl. Multiple overlapping backup products, separate solutions for on-premises and cloud environments, and distinct tools for AI or analytics workloads can create complexity that is costly to operate and difficult to govern.

Ransomware insurance has become an essential component of the risk management toolkit. With 85.6% of respondents already having coverage and 14.1% planning to obtain it, the vast majority of institutions see value in transferring some of the financial impact of cyber-incidents. At the same time, the survey reveals uncertainty. Among those without coverage, half cite complexity and ambiguity of terms as key barriers. Even among insured firms, only 78% report full coverage, with the remainder relying on partial or conditional policies.

This dynamic underscores a critical point. Insurance can help manage financial exposure, but it does not prevent operational disruption, regulatory scrutiny, or reputational damage. It also does not guarantee payouts if firms cannot demonstrate that appropriate controls and recovery procedures were in place. As insurers tighten underwriting standards, institutions with fragmented data protection architectures, weak immutability, or untested recovery plans may face higher premiums, lower limits, or stricter conditions.

IDC expects financial institutions to respond by rationalizing their data protection portfolios. Instead of maintaining multiple point solutions, many will look for platforms that can span on-premises, hybrid, and cloud-native environments; support AI workloads; and offer integrated policy management. The goal is not simply to reduce license counts; it is to create a more coherent control plane that improves visibility, enables consistent enforcement, and reduces the risk of gaps between systems.

In this context, the partnership between Commvault and AWS will often be evaluated on its ability to deliver both technical and economic benefits. Institutions will look for evidence that the combined solution can simplify operations, reduce duplication, and provide clear metrics that link investment in data protection to improvements in resilience and compliance readiness. Those who can tell this story credibly will be better positioned to defend budgets and demonstrate value to boards, regulators, and shareholders.

The Commvault + AWS advantage

The survey results show that financial institutions live in a hybrid world, with critical workloads spread across on-premises infrastructure and AWS-based cloud services.

In this environment, the value of Commvault and AWS lies less in a single feature and more in their ability to provide a unified approach to protection and recovery, consistent protection, visibility, and recovery processes across a distributed estate without forcing teams to manage different tools and operating models in each environment. Rather than managing separate tools for legacy systems, virtualized environments, and modern applications, institutions can use a common platform that understands the full topology of their data estates. This reduces operational friction and helps ensure that policies are applied consistently, regardless of where data resides.

Continuous discovery and automated protection are increasingly important in AWS. Cloud environments change daily as accounts, services, and workloads are created across business units, including cloud-native services (such as Amazon EC2, Amazon RDS, Amazon DynamoDB, and Amazon S3). Commvault Cloud is designed to continuously discover workloads across an organization's AWS footprint and apply or recommend protection policies based on workload type and prior patterns, helping reduce the risk that new services are left unprotected or that policies drift over time. This approach

also complements data classification and tagging efforts by making it easier to connect protection policies to data sensitivity and service criticality.

Faster, cleaner recovery is the second differentiator that buyers increasingly demand. When an incident occurs, speed matters, but so does the hard-won confidence that recovered systems are clean. In addition to immutable copies, many organizations are adopting isolation practices that restore to a separate environment for validation and staging. In the Commvault + AWS context, Commvault Cloud highlights capabilities such as Cleanroom Recovery, which provides isolated recovery environments using AWS on-demand scale for forensic analysis or cyber-recovery or staging validated restores before production recovery. Within or alongside these environments, AI-enabled threat scanning helps detect malware and anomalies in backups, Cleanpoint Identification pinpoints the last known clean recovery point, and Synthetic Recovery accelerates the assembly of clean restore sets. These patterns can reduce the time and uncertainty associated with rebuilding critical services after a cyber-event.

The protection and recovery of AI data foundations is emerging as a new requirement. As firms deploy AI models in production, the supporting assets (e.g., training datasets, feature stores, vector databases, model artifacts, and associated metadata) become part of the critical dependency chain. They must be protected, versioned, and recoverable with the same rigor applied to traditional databases and file systems. In AWS environments, this often means ensuring that the data pipelines feeding AI services, and the stores that power retrieval-augmented generation, are included in backup and recovery plans alongside application workloads. Architectural flexibility and enterprise scale also influence platform selection. Commvault's architecture is designed to disaggregate the control plane from the data plane and remain independent of the underlying storage, enabling deployment as SaaS, software, or hardened appliances depending on where data resides and how it must be operated. For large financial institutions, this flexibility can support consolidation toward a single control plane while scaling the data plane to meet performance and recovery demands, including leveraging elastic AWS compute for burst recovery needs and placing protection capacity close to on-premises or edge data when required. Finally, aligning these capabilities with regulatory frameworks and resilience KPIs connects technology to business outcomes. Financial institutions are measured on their ability to maintain critical services, recover within defined timeframes, and demonstrate the integrity and locality of their data at enterprise scale. Architecturally flexible solutions that combine continuous discovery, policy-driven protection, isolation for validation, and clear reporting complemented by full-stack security integration, such as the Commvault and AWS solution, can help institutions translate resilience investments into measurable outcomes such as tested RTO/RPO, repeatable recovery exercises, and defensible evidence for auditors and regulators.

Challenges and opportunities

The landscape in which Commvault and AWS operate is inherently complex. Financial institutions must manage diverse workloads spanning systems, distributed applications, and modern microservices. They must protect structured and unstructured data, real-time streams, batch feeds, and archival records. They must also support multiple personas, including infrastructure and security teams, data scientists, and application owners. Each of these groups brings different requirements and expectations. A platform that can coordinate protection and governance across this variety must be both technically sophisticated and operationally accessible.

This complexity is not merely technical. It also reflects organizational structures and historical decisions. Many data protection environments bear the imprint of past mergers and acquisitions, regulatory responses, and tactical investments. As a result, institutions may have several backup products, separate solutions for different business lines, and a range of bespoke scripts and processes. Rationalizing this environment can be challenging, but at the core, it is an opportunity. Firms that converge on a smaller set of strategic platforms can reduce operating overhead and gain a clearer view of their risk posture.

Firms that converge on a smaller set of strategic platforms can reduce operating overhead and gain a clearer view of their risk posture.

The survey suggests that data estates supporting AI initiatives are largely already built on AWS. This is consistent with broader trends. Many institutions experiment and scale AI workloads first in the cloud, taking advantage of elastic compute, managed services, and access to modern tooling. Over time, a subset of these initial experiments evolves into production systems that interact with core banking and trading processes.

When this happens, data protection and governance requirements increase. AI workloads become part of the same resilience conversation as payment systems and trading platforms.

For Commvault and AWS, this presents a significant opportunity. If AI workloads already run on AWS, integrating them into existing data protection and governance frameworks becomes a natural next step. Institutions can use Commvault to extend immutability, backup, and recovery to AI data stores, and they can use AWS capabilities to enforce regional boundaries and security controls. This integration can help close the gap between AI innovation teams and central risk functions, which often operate on different timelines and with different vocabularies.

At the same time, the pace of AI innovation means that architecture choices and best practices will continue to evolve. New model hosting patterns, data pipelines, and safety techniques will emerge. Platforms that are too rigid may struggle to keep up. The challenge for Commvault and AWS is to provide a stable foundation for protection and governance while remaining flexible enough to support new AI usage patterns. Institutions will look for evidence of ongoing investment, alignment with road maps, and the ability to support emerging workloads without requiring wholesale redesigns.

Strategic recommendations

IDC recommends that financial institutions take a structured, platform-centric approach to data protection and AI governance readiness. The priority is to ensure that immutability, isolation, and recovery capabilities are robust across both hybrid and cloud-native environments.

Firms should identify their most critical services, map the data flows that underpin them, and confirm that protected copies exist in secure locations with tested recovery playbooks, including procedures for identifying clean recovery points and restoring in isolation where needed. This assessment should cover on-premises systems, AWS-based workloads, and AI data pipelines. Platforms that can enforce consistent policies, continuously discover new workloads, and provide clear reporting across all these domains should be favored.

AI governance readiness requires integrated data controls that extend beyond individual applications or model deployments. Institutions should define common policies for data classification, access, retention, and use for AI training and inference and ensure that these policies are consistently implemented across production, analytics, and backup environments. Logging and observability are essential, since regulators will increasingly

expect firms to show not only that policies exist but that they are applied consistently, monitored, and adjusted when needed. Aligning AI governance efforts with existing data protection and operational resilience programs can help avoid duplication and gaps.

Cloud-native solutions play an important role in scalability and compliance. By using AWS services as foundational components, institutions can utilize built-in encryption, regional isolation, identity and access management, and monitoring capabilities. When combined with Commvault, which can orchestrate backup, recovery, and classification across these services and on-premises systems, firms can build architectures that scale with demand while still meeting strict control requirements. The key is to design with portability and transparency in mind so that critical data and workloads can be moved, recovered, or reconfigured as regulations and business needs change.

IDC recommends that financial institutions consider strategic partners, such as Commvault and AWS, to achieve unified protection, governance, and modernization. While standalone tools have their place, IDC's research supports the conclusion that firms are well advised to identify a small number of platforms that form the backbone of their data resilience strategies. When evaluating platform solutions, buyers should ask how well their solutions support their specific hybrid patterns, how they integrate with existing security and monitoring stacks, and how they will evolve to cover emerging AI workloads. They should also look for evidence of successful deployments in comparable institutions, including demonstrable improvements in recovery performance, regulatory readiness, and operational efficiency.

Ultimately, the institutions that succeed will be those that treat data protection and AI governance readiness not as compliance obligations but as core enablers of digital strategy. Platforms such as Commvault and AWS can help translate this mindset into operational reality, provided they are implemented with clear objectives, strong sponsorship, and ongoing measurement.

Conclusion

Financial institutions are moving through a period of structural change in how they manage, protect, and govern data. IDC research concludes that hybrid estates are now the norm.

Cloud-native workloads sit alongside long-standing on-premises platforms, and AI systems increasingly rely on sensitive financial and customer data. Meanwhile, regulators expect more detailed evidence of resilience and control, and boards expect technology investments to produce measurable risk reduction and support innovation.

The survey results in this paper show that many organizations have taken the necessary steps. Immutability is widely adopted for critical datasets. Cross-region recovery has proven to be effective for most respondents. AI guardrails such as governed retrieval and prompt logging are becoming standard practice. Ransomware insurance is common, and cyber-recovery vaults are in production at many firms that have responded to data localization requirements.

Yet the findings also highlight persistent gaps. Not all institutions have tested recovery across their full hybrid estates. AI governance is not yet fully integrated with broader operational resilience frameworks, and many leaders lack confidence in their ability to

demonstrate AI control effectiveness to regulators. Data protection spending is high, but tool sprawl and architectural complexity can dilute the impact of that investment.

IDC believes the path forward lies in consolidating around a unified platform provider that spans hybrid and cloud-native environments, supports AI workloads, and aligns directly with regulatory expectations. Commvault and AWS together provide one such path. By combining AWS global infrastructure, native services, and security capabilities with Commvault's data protection, classification, and recovery features, institutions can move toward a more coherent control plane for their most important data.

For financial institutions, the next phase will involve turning intentions into consistent practice. This means conducting honest assessments of current resilience, closing gaps in immutability and recovery coverage, extending protection and governance to AI data stores, and, where possible, simplifying architectures. It also means engaging partners that can help translate regulatory requirements, business objectives, and technical realities into a practical, sustainable approach.

Institutions that take these steps will not eliminate risk, but they will put themselves in a stronger position to manage it. They will be better able to withstand disruption, respond to cyber-incidents, and explain their decisions to regulators, customers, and shareholders. As data volumes grow and AI becomes more deeply embedded in financial services, these capabilities will be a key differentiator between firms that keep up and those that use resilience and governance as foundations for long-term competitiveness.

About the IDC analysts

Christopher Lee Marshall

Vice President, Data, Analytics, AI, Sustainability, and Industry Research

Chris Marshall is a vice president responsible for several areas of research at IDC. Marshall leads the Asia/Pacific regional industry research teams, which includes coverage of healthcare, government, retail, energy, manufacturing, and financial services. Additionally, Marshall leads regional teams in data, analytics, artificial intelligence (AI), future of work, and sustainability.

More about Christopher Lee Marshall →

Jerry Silva

Program Vice President, Financial Insights, IDC

Jerry Silva is program vice president for IDC Financial Insights, leading the Global Financial Services Research programs across banking, insurance, and capital markets. He draws on 40+ years of experience in the financial services industry covering a variety of topics, from digital infrastructures to AI, data management, and IT governance.

More about Jerry Silva →

IDC Custom Solutions

IDC Custom Solutions produced this publication. The opinion, analysis, and research results presented herein are drawn from more detailed research and analysis that IDC independently conducted and published, unless specific vendor sponsorship is noted. IDC Custom Solutions makes IDC content available in a wide range of formats for distribution by various companies.

IDC.com | IDC on LinkedIn | IDC Blog

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications, and consumer technology markets. With more than 1,300 analysts worldwide, IDC offers global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries. IDC's analysis and insight helps IT professionals, business executives, and the investment community to make fact-based technology decisions and to achieve their key business objectives.