DELL Technologies

Modernizing financial services at scale with full control

Practical technology approaches that community and regional banks, credit unions, and insurers can use to balance growth, governance and limited resources in highly regulated environments.

intel

Windows 11

Executive summary

Banking and financial services organizations are operating in increasingly digital-first environments. As transaction volumes continue to grow, data spans more systems while expectations for availability, security and compliance remain high. To keep pace, many must update their technology estates — from desktops to the edge and core to the cloud — and ensure their systems are fully capable of meeting not only today's demands but also tomorrow's.

For financial services providers, these pressures are compounded by limited resources for the IT teams that manage supporting systems and by no allowance for disruptions. At the same time, IT management must show that their modernization efforts, including AI deployments, can produce measurable operational results and deliver real returns on investment.

This paper suggests the most important outcomes to consider for updating systems and making them future-ready include: confidence in digital operations and transactions; scalable risk management and compliance; built-in resilience; well-governed decision-making; and increased productivity for highly focused teams. It also explores the barriers that often slow progress, including legacy infrastructure, fragmented environments, regulatory complexity and operational strain.

Rather than addressing such challenges by themselves, organizations are advised to consider integrated approaches that align infrastructure, data, devices and intelligent capabilities, so they can modernize in a stepwise approach without increasing risk.

Modernization's core goals should be to enhance their ability to operate more efficiently as demand grows, maintain control as environments become more complex, and always deliver exceptional digital experiences to delight customers and reinforce their trust.

Modernizing infrastructure to drive digital-first growth

Digital-first delivery of banking and financial services is no longer a differentiator. For many institutions, it's the default operating model for customer transactions and interactions in response to rising market expectations. In a 2025 American Banking Association survey of 4,400 adult banking customers spanning all age groups, 76% said they prefer managing their accounts via mobile apps or online web access.[1]

This is why payments, account servicing, lending workflows and advisory services now depend on systems that must operate continuously, securely and at scale. But for financial services providers, this shift requires that they strike a delicate balance in deploying technology.

Managing tradeoffs. While digital channels can enable more efficient, higher-margin operations, they can also increase exposure to security and disruption risks. As transaction volumes rise and data moves across more systems, the margin for error widens. Outages, latency or security lapses can quickly undermine customer trust and regulatory compliance.

In all their operations, banking and financial services institutions must demonstrate control, auditability and consistency across increasingly complex environments. That pressure is compounded by lean IT teams, legacy infrastructure and technology estates that have grown incrementally rather than strategically.

Simplifying complexity. For financial services providers, the result can be a widening gap between what digital-first operations demand and what their IT environments were designed to support at scale. This includes long-established firms or new entrants with platforms they built cloud-native from day one.

Systems optimized for predictable workloads increasingly face more dynamic processing volumes, higher data intensity, and tighter expectations around performance and governance. Point upgrades or isolated fixes may address immediate symptoms, but they often add complexity rather than reduce it.

In this context, modernization is less about speed and more about stability. Banking and financial services leaders need to prioritize approaches that strengthen resilience, reduce fragmentation and silos, and support digital growth without increasing operational or regulatory risk.

The challenge is not whether to modernize, but how to do so in a way that reinforces customer and regulatory confidence — in systems, decisions and user experiences — at every stage of the journey.

Priority outcomes for banking and financial services providers

Technology modernization should provide practical outcomes that enhance daily operations, regulatory posture and customer relationships. Organizations must question whether new technology investments improve reliability, strengthen oversight and support growth without adding complexity or risk.

For financial services providers, top-ranked outcomes are achieved through technology investments that strengthen the organization without introducing new risk exposures. Here are key outcomes to consider:

Scale digital-first experiences and operational capacity with confidence
Support rising volumes of digital activity — accounts, payments, data exchanges and customer interactions — while enabling more personalized, context-aware experiences without compromising service availability, system performance or customer trust.

Reduce risk and enhance compliance
Maintain governance, security and auditability as environments become more distributed and interconnected, without introducing operational friction or obscuring accountability.

Build resilience into everyday operations
Treat resilience as a bedrock design principle, so systems can adapt to changing loads, isolate issues and recover quickly when disruptions occur.

Support faster, better-informed decisions
Let teams act on more timely, contextual insights, supported by analytics or AI, while preserving transparency, auditability and regulatory compliance.

Amplify the efforts of focused IT teams
Reduce manual activities and interventions, simplify management, and minimize context switching so staff time and expertise are directed toward higher-value work rather than maintaining unnecessary complexity.

Taken together, these outcomes can define success for digital-first service delivery. The challenge lies in achieving them simultaneously, without trading rapid implementation and commissioning cycles for continued operational stability, security and control.

Barriers to digital-first progress in banking and financial services

While many banking and financial services providers intend to modernize or scale, they may face limitations imposed by the assumptions embedded in their IT environments.

For example, whether they built their systems over decades or more recently developed cloud-native ones to support core banking, payments, compliance and customer interactions, those systems may well have been designed around predictable workloads and narrower integration requirements. However, as digital channels expand and transaction volumes rise, those assumptions may no longer hold.

Legacy infrastructure can compound this problem. Core systems must remain critical and stable, but they are frequently surrounded by layers of newer tools added to address specific needs. Over time, this results in environments that are harder to manage, monitor and adapt. Changes in one area can have unintended consequences elsewhere, increasing operational risk.

Unwanted complexity. In response, organizations often turn to point solutions for solving immediate problems: fraud detection, analytics, performance monitoring or customer engagement. Although each solution may be effective on its own, they are often grafted onto existing systems without a unifying architectural approach.

Modern core infrastructure for digital operations

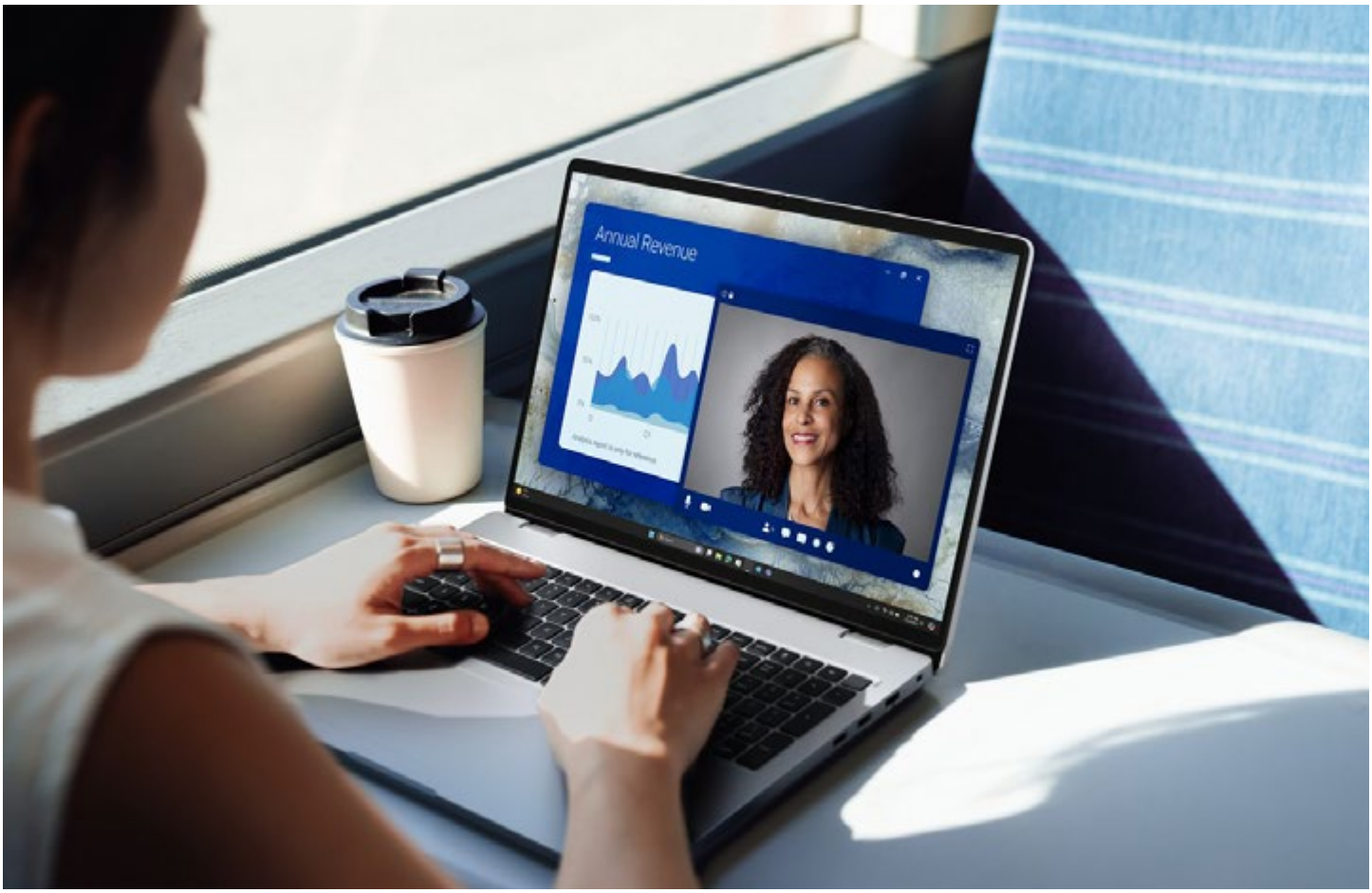
Modern compute and storage platforms provide a resilient foundation for transaction processing, data management and application performance.

Dell PowerEdge servers, powered by the latest Intel® Xeon® Scalable processors, deliver advanced security features such as Intel® Software Guard Extensions (SGX) and Intel® Total Memory Encryption, helping financial institutions protect sensitive data and meet regulatory requirements.

Designed to evolve incrementally, these environments support availability, governance and scalability as workloads become more distributed — whether deployed on premises, in hybrid cloud configurations or consumed through flexible, consumption-based models.

Banks and financial service providers can modernize their core infrastructure by taking advantage of the following Intel®-based Dell platforms coupled with Microsoft's Windows Server and Azure hybrid services:

- **Dell PowerEdge servers:** Core compute for transaction processing, virtualization, databases and regulated workloads. With Intel® Xeon® 6 processors, PowerEdge servers handle data-heavy workloads with ease, maintaining speed and reliability when it matters most.
- **Dell PowerStore/PowerMax storage:** High-performance, resilient storage for core banking systems, payments platforms and data-intensive workloads.
- **Dell APEX (as-a-service infrastructure):** Consumption-based infrastructure that allows institutions to modernize incrementally without large upfront investments.



As a result, point solutions can introduce new dependencies, management overhead and data silos, making the overall environment more complex rather than more resilient. And third-party solution providers can introduce new security vulnerabilities that need addressing.

Regulatory pressure further complicates this picture. Institutions must demonstrate visibility, auditability and control across systems that weren't designed to operate as a cohesive whole. When data and processes are fragmented, proving compliance becomes more labor-intensive and prone to errors.

Staffing realities. At the same time, workforce constraints limit how much complexity organizations can handle. Many institutions operate with core IT teams responsible for maintaining availability, security and performance while also supporting ongoing change. As environments become more fragmented, routine tasks consume more time, leaving less capacity for strategic work.

Together, these factors create a reinforcing cycle. Legacy systems constrain change, point solutions add fragmentation and limited resources make simplification difficult. Breaking that cycle requires approaches that reduce complexity at the foundation, rather than adding another layer on top of it.

Integrated approaches to modernization are best

As banking and financial services organizations modernize, many discover that incremental improvements alone are not enough. Over time, environments shaped by point solutions — added to address specific risks, compliance needs or performance gaps — become harder to manage as a whole. Each tool may solve a specific problem, but collectively they can increase fragmentation, limit visibility and consume operational capacity.

An integrated approach addresses this challenge by focusing on optimizing how core systems, data, security controls and user environments work together. Rather than layering new capabilities onto existing complexity, integration simplifies how environments are monitored, governed and developed. This reduces the operational burden associated with managing multiple tools and improves consistency across systems.

From a resilience perspective, integration enables clearer insight into dependencies and potential failure points. When systems are designed to interoperate seamlessly, issues can be identified earlier and addressed faster and more effectively. Recovery becomes faster and more predictable because teams are working in a unified operational framework rather than coordinating across disconnected platforms.

Security and governance also benefit from integration. Policies can be applied more uniformly, audit trails are easier to maintain and compliance reporting becomes less burdensome. Instead of reconciling data from multiple sources, teams can gain a more complete and trustworthy view of how controls are functioning across their IT environments.

Finally, integration supports productivity for core IT teams. Simplified management, fewer handoffs and clearer visibility reduce time spent on routine maintenance and troubleshooting. That reclaimed capacity allows teams to focus on higher-value work, including improving services and supporting growth.

Collectively, technology integration creates a foundation that supports resilience, security and productivity simultaneously — without requiring disruptive changes or constant interventions as digital-first operations continue to grow.

Applied AI and analytics for operations and decision support

Governed AI and analytics platforms enhance monitoring, pattern detection and situational awareness across digital environments. Integrated with core systems and security controls, these capabilities support fraud detection, operational insight and decision support without sacrificing transparency or auditability.

Hybrid approaches that span on-premises, Intel-powered Dell solutions with Windows 11 and Microsoft Azure environments allow institutions to scale AI and analytics cost-effectively as needs evolve.

- **Dell AI Factory:** A portfolio approach combining infrastructure, software and services to support governed AI workloads.
- **Dell PowerEdge + accelerated compute:** For fraud detection, anomaly monitoring and analytics.
- **Hybrid AI architectures:** Supporting analytics across on-prem, edge and cloud environments.

Applying AI in practical, well-governed and accountable ways

Interest in analytics and AI continues to grow across banking and financial services as organizations look for better ways to enhance the customer experience, especially with personalization, while improving efficiencies and margins. Given these potential benefits, many institutions have accelerated implementations of AI-driven automation models. In fact, NVIDIA's annual survey of 600 global financial services professionals reported that nearly all planned to increase spending on AI infrastructure.[2]

However, the industry has good reason to be cautious, especially regarding cybersecurity. Accenture's annual survey of 600 banks worldwide found that 83% reported difficulty in aligning security with AI adoption.[3] And with AI-enabled threat actors on the rise, that flaw can create risks to customer trust and regulatory compliance.

In regulated environments, the value of AI can be inseparable from the ability to apply it with transparency, control and accountability. However, its effective implementation isn't clear for most institutions: 70% of banks, for example, are concerned about regulatory scrutiny in deciding whether to use AI in credit modeling.[4]

Realizing AI's potential. For many institutions, AI delivers the most value when it is embedded into existing operations rather than introduced as a standalone initiative. Applied carefully, analytics and AI can support monitoring, anomaly detection and decision support across areas such as fraud prevention, underwriting, compliance and operational performance — without displacing human judgment or established controls.

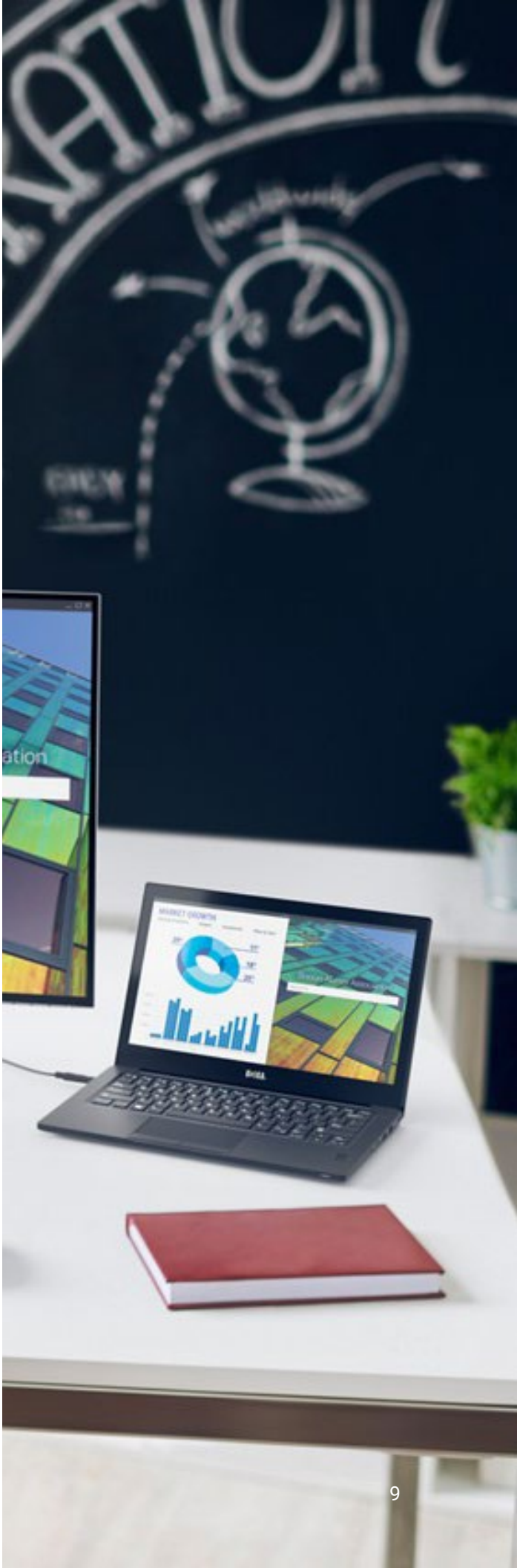
These realities reinforce the need for AI systems that produce transparent, auditable outputs and operate within clearly defined governance frameworks. While AI can automate workflows for greater efficiencies, reduced costs and more customer responsiveness, it can also improve situational awareness and operational visibility for faster issue resolutions.

For example, teams can gain insights much sooner into emerging issues, get faster access to relevant information to address or mitigate them, and better understand how to prevent their recurrence. This is especially important for institutions with limited staff, where AI can help reduce manual effort without introducing opaque or hard-to-defend outcomes.

Edge infrastructure matters. The choices organizations make about where and how AI workloads run shape how responsibly those capabilities can be applied. Processing data closer to where it is generated can reduce latency, limit unnecessary data movement, and simplify security and compliance oversight.

When AI capabilities are integrated with core systems and operational controls, they scale more predictably as digital activity increases. Intel® Xeon® Scalable processors with built-in AI acceleration, such as Intel® Deep Learning Boost, enable banks to run AI workloads for fraud detection and compliance monitoring efficiently on premises, reducing latency and supporting real-time decision-making.

In banking and financial services, AI adoption is most effective when it reinforces trust, governance and day-to-day operational confidence. Applied within well-governed environments, intelligent capabilities can enhance awareness, efficiency and resilience — while preserving the ironclad trust that customers and regulators expect.



Supporting the people behind the systems

Digital-first banking places sustained demands on the people responsible for keeping systems available, secure and compliant. For many community and regional institutions, those responsibilities fall to IT teams managing increasingly complex environments while having to orchestrate ongoing changes, often with limited resources.

As systems become more distributed and interconnected, the cost of complexity is often borne by staff. Fragmented tools, manual processes and constant context switching increase workload and reduce the time available for higher-value work. This strain can limit responsiveness and make it harder to maintain confidence in daily operations.

More visibility. Modernization efforts that simplify environments help relieve this pressure. When infrastructure, security controls and management tools are better aligned, teams gain clearer visibility into system health and risks. Routine tasks require less manual effort, and staff can address issues much earlier, before they escalate.

Importantly, this approach does not remove people from the equation. Instead, it supports informed human oversight by reducing noise and surfacing relevant information more effectively. Staff are better equipped to make decisions, respond to incidents and support customers without being overwhelmed by complexity.

By improving how work is supported — not just what systems can do — institutions create more sustainable operating models. Teams remain effective as digital activity grows, helping organizations maintain reliability, compliance and service quality over time.

Integrated client endpoint and workspaces for team members

Secure, manageable endpoints and workspace platforms help extend reliability from the data center to the people supporting customers every day. By aligning devices, identity, access controls and management tools, institutions can reduce operational friction, improve consistency and support secure work across roles and locations.

Secure, manageable endpoints and workspace platforms help extend reliability from the data center to the people supporting customers every day. By aligning devices, identity, access controls and management tools, institutions can reduce operational friction, improve consistency and support secure work across roles and locations. As endpoint environments grow more distributed, automation and centralized orchestration become critical to maintaining control, accelerating deployment and enforcing security standards at scale.

With Windows 11 aboard and Microsoft device-management services to simplify deployment and lifecycle management, these Dell endpoints can help boost staff productivity and responsiveness:

- **Dell Pro laptops and desktops:** Secure, manageable endpoints for frontline, operations and support staff. Dell Latitude and OptiPlex PCs with Intel® vPro® platform provide hardware-based security, remote manageability, and performance for banking staff — ensuring compliance and productivity across distributed teams.
- **Dell Pro Precision workstations:** Powerful, secure performance for analytics, modeling and AI-assisted workflows at the point of work, helping teams process complex data locally with confidence.
- **Dell Trusted Workspace and Management Solutions:** Centralized device deployment, security and lifecycle management.
- **Dell NativeEdge and Dell Automation Platform:** Centralized orchestration and automation capabilities that simplify endpoint and edge environment deployment, configuration and security. These platforms help IT teams standardize operations, reduce manual effort and maintain governance as they scale their environments.
- **Dell thin client solutions:** Useful for call centers, branches and task-based roles.

AI-enabled end-user devices

AI-capable PCs can bring intelligent assistance closer to staff and data sources, supporting analytics, automation and productivity at the point of work.

- **Dell Pro laptops and desktops:** When paired with Intel-based AI acceleration and Windows 11 experiences such as Microsoft Copilot+, these powerful PCs can help employees and teams work more efficiently while maintaining local data control and security.
- **Dell Pro Precision laptops and desktops:** These Intel-powered, high-performance PCs with Windows 11 and Microsoft Copilot+ can tackle even more demanding AI workloads, including analytics and machine learning.

Building confidence for what comes next

IT modernization depends less on adopting individual technologies and more on how systems, data and people are brought together. Fragmented environments, shaped by years of incremental change, can make it harder to manage risk, demonstrate control and support core IT teams. By contrast, integrated approaches simplify oversight, reduce operational friction and create a more stable foundation for digital-first operations.

This is especially important as intelligent capabilities, especially analytics and AI, become more common. When applied within well-governed IT environments, these tools can enhance visibility, expedite support, facilitate better-informed decisions, and improve efficiency without undermining transparency or accountability. Infrastructure and deployment choices play a critical role in ensuring that intelligence scales responsibly as digital activity grows.

Equally important is how modernization supports the people behind daily operations. Simplified environments, clearer visibility and reduced manual effort allow teams to focus on higher-value work — maintaining reliability, responding to issues and supporting customers — rather than managing complexity.

Taken together, these considerations point toward a pragmatic path forward. By modernizing incrementally, aligning systems and controls, and embedding intelligence within governed operations, banking and financial services organizations can strengthen resilience, improve performance and support growth without disruption. The result is an operating model that is better equipped to meet today's demands as well as adapt confidently to what comes next.

Use case: Scaling digital transactions without increasing operational risk

As community and regional financial institutions grow, their digital transaction volumes are steadily rising. Online banking usage expands, payment activity increases and additional third-party services are introduced to support customers.

For IT teams with limited resources, the challenge is enabling growth without introducing instability, performance issues or new points of failure.

By modernizing core systems in stages, institutions can accommodate higher transaction volumes while maintaining consistent performance and availability.

Integrated technology enables end-to-end operational visibility that helps teams identify capacity constraints early and address them before customers are affected. Because improvements are introduced incrementally, daily operations remain stable and regulatory compliance continues to be met.

The result is growth that feels manageable, not precarious. Transactions increase, systems remain dependable and teams remain confident the environment can support future demand without added risk.

Use case: Improving compliance visibility and audit readiness across hybrid environments

A credit union operating across on-premises systems, cloud platforms and third-party applications faces growing complexity in managing security, controls and data. While individual systems may perform well, maintaining consistent compliance oversight across the full environment becomes increasingly difficult, particularly with limited staff and frequent audits.

By aligning infrastructure, security controls and governance more closely, the organization gains clearer, end-to-end visibility. Policies are applied consistently, audit trails are easier to maintain and compliance reporting requires less manual effort. Instead of spending time reconciling information across disconnected tools, teams can focus on preparation and oversight.

The results are a lighter day-to-day compliance burden and stronger confidence from regulators. As the environment evolves, governance keeps pace, allowing the institution to modernize without sacrificing transparency or control.

Use case: Enabling faster, well-informed decisions for operations and frontline teams

A regional insurance agency supports customer service, underwriting and claims operations with a highly focused, core IT team responsible for monitoring end-user client devices, infrastructure health and issue response. As data volumes increase, manual review alone becomes time-consuming and can slow resolutions when problems emerge.

By using analytics and decision-support tools within existing systems and controls, the agency improves visibility into operational activity. Patterns and irregularities are flagged early, helping staff focus attention where it matters most. Because insights are explainable and reviewed by people, decisions remain accountable and aligned with compliance requirements.

This approach improves efficiency without replacing judgment. Teams spend less time sorting through data and more time addressing real issues, improving responsiveness and maintaining the oversight required in regulated financial environments.

By modernizing incrementally and aligning systems, governance, and intelligent capabilities, banking and financial services organizations can translate operational discipline into sustained market advantage—moving faster where it matters, staying firmly in control and consistently delivering stand-out experiences customers can trust.

To learn more, visit Dell.com/Industries

1. American Bankers Association, National Survey: Bank Customers Continue to Use Mobile Apps More Than Any Other Channel to Manage Their Accounts, November 18, 2025.
2. NVIDIA, State of AI in Financial Services: 2025 Trends.
3. Accenture, Guardians of Trust: Navigating Cybersecurity in Banking, March 2025.
4. Ron Shevlin, Achieving High-Performance Lending: The Impact of AI on Lending Efficiency, Cornerstone Advisors, 2024.

This white paper is for informational purposes only and may contain typographical errors and technical inaccuracies. The content is provided as is, without express or implied warranties of any kind.

Copyright © 2026 Dell Inc. or its subsidiaries. All Rights Reserved. Dell Technologies, Dell and other trademarks are trademarks of Dell Inc. or its subsidiaries. Other trademarks may be trademarks of their respective owners. Other names and brands may be claimed as the property of others.

DELL Technologies