Risk, resilience, and the modern financial workspace

How financial organizations can reduce risk, control costs, and build a resilient IT foundation

omnissa®

The hidden risk of standing still

Financial services has always operated at the intersection of trust and complexity, but today the stakes are higher. The workforce is hybrid by default. Regulators—from FFIEC to DORA—increasingly require not just documentation, but proof of resilience. Cyber threats are increasing in sophistication and frequency. And audit teams now expect continuous control evidence, not periodic snapshots.

Many legacy virtual desktop and endpoint platforms mask risk through familiarity. Manual processes, inconsistent policy enforcement, and limited visibility create hidden exposure—often uncovered only during audits or incidents. Rising costs may be the first sign, but the deeper issue is unmeasured operational risk.

For IT leaders, modernization isn't simple. Cost pressures, regulatory demands, disruption concerns, and sunk investments slow progress—even as aging systems strain under growing workloads and compliance expectations.

Over time, the status quo becomes harder to defend. Overhead rises, control gaps widen, and agility declines just as the business needs greater resilience and speed. Modernization shifts from optional to inevitable.

The challenge is building alignment—advancing solutions that reduce risk, improve auditability, control costs, and enable secure growth. This guide helps institutions recognize when legacy workspace technologies are holding them back—and how to build a clear, defensible case for change.

Standing still isn't neutral. In financial services, inaction is risk.

Exposure hidden in plain sight

Compliance exposure you may not be measuring

Regulatory frameworks like FFIEC, GLBA, PCI-DSS, DORA — now require demonstrated operational controls and not just documented policies. Examiners ask to see how controls are enforced in practice, how quickly anomalies are remediated, and how the organization would demonstrate continuity under adverse conditions.

Legacy platforms struggle here. Periodic scanning creates visibility gaps. Manual enforcement processes produce inconsistency. Fragmented audit trails make it impossible to respond to regulators on short timelines. Beyond direct fines, remediation burdens often cost multiples of what proactive modernization would have required.

What's hidden in plain sight

Legacy platforms carry a growing maintenance burden: hardware refresh cycles, complex image management, performance limitations, and infrastructure costs that are increasingly difficult to justify. Every day that endpoint controls cannot be continuously verified produces audit exposure. In an era of real-time regulatory expectation, periodic compliance is no longer sufficient.

Ransomware, credential theft, and supply chain compromises are expected features of the operating environment, not exceptional events. And attackers are sophisticated at exploiting exactly the weaknesses that legacy environments produce: unpatched endpoints, inconsistent policy enforcement, delayed detection of lateral movement.

When legacy platforms increase risk and undermine resilience

The biggest mistake in modernization planning is positioning it as a tech upgrade. Boards evaluate investments through cost and risk, so the stronger case frames it as improving risk management and operational resilience.

An effective plan starts with a clear view of your current state:

- What percentage of endpoints are consistently compliant, and how is that verified?
- How quickly are policy violations on remote endpoints detected?
- What's the mean time to patch critical vulnerabilities?
- Could you demonstrate today that endpoint controls are operating as designed?

In banking, insurance, and capital markets, risk builds quietly. Legacy desktop and application platforms, marked by slow response, limited visibility, and inconsistent controls, degrade over time. These issues escalate during audits, incidents, or renewals, when rising costs collide with growing regulatory exposure.

The impact goes beyond IT budgets. It raises tougher questions: Why is audit effort increasing while visibility remains fragmented? Why does incident response depend on manual workarounds? Why do controls that look sound on paper fail under scrutiny?

Platforms that once felt stable become sources of hidden risk—undermining resilience just as regulators and the business demand stronger assurance and faster response.

Why financial organizations hesitate

Risk aversion and reliance on legacy systems
Stability often outweighs change in regulated environments. Legacy systems feel safer because they're familiar and approved—even when they rely on manual workarounds. As a result, new approaches can seem riskier, even when the real risk is sticking with the status quo.

Operational and organizational impact of change
Technology changes in financial institutions have broad ripple effects—impacting processes, controls, training, and governance. Without a clear link to reduced risk and stronger resilience, stakeholders often see the disruption as outweighing the benefits.

Uncertainty around outcomes and audit impact
When modernization benefits aren't clearly defined or measurable, institutions delay. Without evidence of stronger controls or resilience, they default to short-term certainty—even as long-term risk grows.

omnissa

Build a defensible, audit-ready plan

A strong modernization plan starts with audit readiness—clearly showing where controls exist, how consistently they're enforced, and how quickly evidence can be produced.

The first step is identifying where manual processes, fragmented tools, or limited visibility weaken audit confidence. These gaps often go unnoticed until audits or incidents reveal missing evidence, inconsistent enforcement, or slow response. A defensible plan aligns IT, risk, and compliance around improving control consistency, evidence quality, and readiness.

Auditors focus on three realities:

Where controls actually break down
Auditors assess execution, not intent. Manual processes, compensating controls, and legacy workarounds increase effort and the risk of findings due to inconsistency or gaps. Documenting these issues clarifies the risk of maintaining the status quo.

Whether controls are applied consistently
Findings often stem from uneven enforcement across teams, devices, or environments. Aligning on shared control objectives and requirements ensures technology decisions address real gaps in visibility, access governance, monitoring, and reporting.

Whether outcomes can be measured and proven
Approval depends on demonstrating improved audit readiness. A strong case highlights reduced manual evidence collection, stronger enforcement, faster response, and repeatable execution—backed by measurable KPIs tied to risk reduction and resilience.

Go deeper:

Tools alone do not make a bank audit-ready. Governance, control and ownership are critical. A modern platform enables those controls to be executed consistently and documented at scale—turning audit readiness from a periodic scramble into an ongoing state.

Evaluating benefits across risk, resilience and operational control

Benefits should be evaluated by how effectively they reduce operational risk, improve audit outcomes, and strengthen resilience. Financial impact still matters—but risk exposure, control effectiveness, and response speed are equally critical to long-term performance and regulatory standing.

As you evaluate challenges with your current solution, take note of the following issues, which often signal growing cost, risk, or operational strain:

- Inefficient or fragmented processes that lead to long turnaround times or elevated mean time to resolution (MTTR).
- Difficulty hiring or retaining talent due to outdated platforms or overly manual operating models.
- A growing backlog of support requests that impacts service levels and frontline productivity.
- IT teams spending disproportionate time on repetitive, manual tasks rather than risk mitigation, modernization, or strategic initiatives.
- Year-over-year cost increases without corresponding improvements in performance or capability.
- Declining satisfaction among IT teams, business users, or both.
- Downtime or performance degradation that affects productivity, customer experience, or regulatory commitments.

Common Indicators of Underperforming Banking Technology

Audit prep takes weeks, not hours. Modern platforms maintain perpetual audit readiness; legacy systems treat every exam like a fire drill.

Security policies don't follow your people. If the controls enforced on the workstation don't apply to the remote laptop or branch device, you have an enforcement gap.

Your IT team spends more time reacting than improving. High help desk ticket volumes from endpoint failure, manual patch cycles measured in weeks, and IT staff consumed by routine remediation rather than strategic work are all symptoms of the same underlying problem.

omnissa

Hard benefits: reducing measurable risk, exposure, and cost

For institutions modernizing with Omnissa, these benefits fall into four key categories.

Reduced breach risk
Omnissa continuously enforces policy across all endpoints, including remote and hybrid workers. Automated patching helps close common attack gaps, while zero trust access uses real-time device posture and behavior to limit lateral movement.

Lower compliance burden
Omnissa shifts audit prep from weeks of manual work to on-demand reporting. Continuous logging of enforcement, exceptions, and remediation provides audit-ready documentation for internal and regulatory reviews.

Infrastructure cost consolidation
Many institutions maintain overlapping endpoint, VDI, and security tools from years of fragmented decisions. Omnissa unifies endpoint management, Horizon VDI, and security into a single platform.

Reduced operational overhead
Legacy environments are labor-intensive. Omnissa helps reduce helpdesk tickets through automated remediation, simplifies application delivery, and enables self-service—lowering ongoing IT support demands.

Assigning financial value to these gains—through cost avoidance, productivity, and reduced third-party reliance—clarifies bottom-line impact. This helps finance, risk, and executive stakeholders see how modernization improves ROI while strengthening long-term discipline.

Success story

Yapi Kredi, one of Türkiye's largest private banks, modernized operations with Omnissa's unified digital workspace to support a distributed workforce and thousands of devices. As it expanded into mobile and digital services, it needed consistent management, strong security, and reliable access to applications. With Workspace ONE and Horizon, the bank centralized endpoint management, increased automation, and strengthened data protection—enabling secure, flexible banking services while maintaining compliance.

Read the case study to learn more.

omnissa

Operational resilience benefits: faster response and reduced disruption

Not every benefit of modernization can be captured in a spreadsheet. In financial services, the ability to maintain operations through cyber incidents, respond to a regulatory request within hours, or recover a compromised endpoint without disrupting critical business functions can be the difference between a manageable event and a material one.

Continuity under pressure

Omnissa enables rapid endpoint reimaging and restoration without physical access which can be essential for distributed workforces. Horizon capabilities help keep critical business applications accessible even when physical endpoint issues occur. And when the platform detects a security anomaly, you can isolate the affected endpoint and initiate remediation without manual intervention at each step.

Faster detection, faster response

Legacy environments detect anomalies through periodic scanning - the window between compromise and detection is measured in hours or days. Omnissa has real-time behavioral monitoring, automated alert enrichment, and integrated response workflows that accelerate time from detection to containment.

Reduced user disruption

For financial services organizations, user disruption has direct business consequences: relationship managers unable to access customer data, traders cut off from critical applications, compliance teams unable to respond to time-sensitive requests. Predictive remediation identifies and resolves endpoint issues before they affect users.

Strategic benefits: regulatory confidence and control maturity

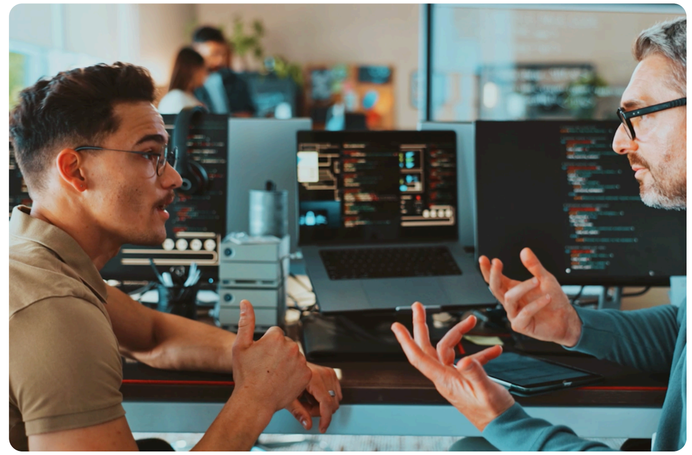
Beyond immediate hard and soft benefits, modernizing with Omnissa produces strategic advantages that compound over time: stronger regulatory relationships, a more mature control environment, and the organizational confidence that comes from genuinely knowing your risk posture.

Financial services examiners have shifted their expectations. The question is not whether you have a policy, but how the policy is enforced continuously, across the entire operating environment. Financial organizations that can answer with real-time compliance dashboards, automated remediation logs, and continuous behavior monitoring data have a fundamentally different examination experience than those relying on manual evidence collection.

Omnissa supports on-demand production of examiner-ready evidence, comprehensive automated audit trails, and rapid closure of control gaps before they become findings.

The most forward-looking strategic benefit is the transition to a continuously auditable operating model where evidence of control effectiveness is generated automatically, maintained continuously and available on demand. This changes not just regulatory posture but the entire approach to IT governance. Internal audit operates in a state of perpetual readiness and board risk committees receive reporting rather than estimates.

The Omnissa platform advantage: reducing risk by design



Omnissa delivers built-in visibility, unified control, and audit-ready evidence across endpoints, apps, and virtual workspaces. Instead of layering tools after the fact, organizations embed resilience into daily operations—reducing risk, effort, and uncertainty.

It's not a bundle of point products, but an integrated platform where endpoint management, VDI, and security work together to share data, enforce policies consistently, and provide unified visibility.

- **Economic advantage** – As costs rise and pricing fluctuates, Omnissa offers a more predictable, cost-effective model. Consolidating capabilities reduces total cost of ownership and eliminates overlapping tools.
- **Flexible licensing** – Broad licensing options align spend to actual needs, improving budget predictability and adapting to evolving workforce and regulatory demands.
- **Technology advantage** – Built-in app lifecycle management, digital employee experience (DEX), and automation improve visibility, accelerate issue resolution, and simplify operations—without added complexity.
- **Platform advantage** – A unified architecture integrates VDI, UEM, DEX, and security, strengthening policy enforcement and delivering consistent controls across users, devices, and locations at lower cost.

By choosing a platform—not just products—financial institutions gain a scalable, resilient foundation for compliance today and future demands.

The question isn't whether to modernize, but whether to act proactively—or react later under pressure. Omnissa provides a proven path to building a resilient workspace.

Modernize your financial workspace with confidence. Reduce risk, improve readiness, and lower costs with a proven, unified platform. Talk to an expert or explore the Omnissa platform.

LEARN MORE