

# Modernizing Financial Services IT: Building Secure, Scalable, and AI-Ready Infrastructure for Real-World Pressures

If you're running IT in a bank, credit union, or insurance organization today, you're balancing more priorities than ever: AI adoption pressure from the business, escalating fraud risk, new cross-border payment deadlines, hybrid cloud modernization, and sweeping regulations such as DORA, Basel 3.1, and the EU AI Act. Meanwhile, your environment spans legacy cores, cloud-native apps, digital channels, agent desktops, and dozens (sometimes hundreds) of branch locations.

You don't need a primer on the financial industry. You need technology and expertise that helps you modernize safely, scale efficiently, and meet compliance expectations without slowing innovation. This paper focuses on the IT challenges you're experiencing right now—and the modernization approaches that strengthen resilience, improve security, and accelerate regulated innovation.



## AI SHIFTS FROM EXPERIMENTATION TO EMBEDDED WORKFLOWS

Across financial services, AI is no longer confined to pilots. Institutions are beginning to deploy AI into daily workflows for underwriting, claims, customer support, software development, and risk analysis. Analyst reports consistently show that AI is now a top focus area for executives. McKinsey has noted that as much as 30% of banking activities have the potential to be automated, and banks are actively trying to operationalize that potential in ways that improve accuracy, reduce operational risk, and accelerate throughput.

But IT teams are finding that AI adoption requires more than standing up a model or an assistant. They must address governance, lineage, transparency, and monitoring in a way that satisfies evolving regulatory expectations. Many organizations are discovering that tracking AI ROI is difficult, particularly as deployments scale, which is increasing pressure to strengthen data foundations, centralize model oversight, and build environments where AI can be deployed safely, consistently, and in ways that directly support business outcomes.

**AI is becoming operational, not experimental.**

*Institutions are moving beyond pilots and need secure, governed environments that support enterprise-grade AI while meeting transparency and compliance requirements.*



## CYBER RISK, FRAUD GROWTH, AND THE MANDATE FOR OPERATIONAL RESILIENCE

Financial services continues to experience some of the highest cybersecurity costs of any sector. IBM's Cost of a Data Breach report highlighted that financial institutions face average breach costs of nearly six million dollars, second only to healthcare. Ransomware attacks targeting banks rose dramatically, with Check Point Research reporting a more than 70% increase. New fraud patterns have emerged through instant payment rails, social engineering, and compromised credentials, increasing the complexity of detection and response.

Regulators have responded by raising expectations around operational resilience. Requirements around stress testing, business continuity, and third-party oversight are expanding. Many institutions are investing in stronger monitoring and observability across cloud and branch systems, adopting Zero Trust identity controls, and segmenting networks to reduce the risk of lateral movement. These efforts are not simply about compliance. They are rapidly becoming table stakes for maintaining customer trust and protecting high value assets.

**Cyber resilience must extend across cloud, branch, and third-party environments.**

*With breach costs near six million dollars and ransomware attacks rising steeply, IT teams must modernize identity, segmentation, and observability.*



## REAL TIME PAYMENTS AND ISO 20022 RESHAPING INFRASTRUCTURE DEMANDS

The shift toward real time payments is accelerating. Institutions operating on RTP and FedNow rails are discovering that instant settlement introduces new infrastructure expectations, particularly around latency, monitoring, and fraud detection. Real time payments reduce friction for customers but compress the time window for identifying suspicious activity. This is pushing IT teams to strengthen their analytics pipelines, improve event correlation across systems, and ensure that high availability architectures can support constant uptime.

At the same time, the industry wide move to ISO 20022 is transforming how payment data must be handled. The transition away from MT messages is forcing updates across payment engines, AML platforms, sanctions screening tools, and downstream analytics environments. Institutions that embrace ISO 20022 data are already seeing improvements in fraud detection and straight through processing because the richer structure enables more precise screening and automation.

***Instant payments require smarter, data-driven systems.***

*Payment systems must be resilient, continuously monitored, and integrated with fraud engines that can act in seconds, not hours.*



## TOKENIZATION AND ON CHAIN FINANCE ENTER PRACTICAL ROADMAPS

Tokenized assets and on chain finance have moved out of lab environments and into institutional planning discussions. Major asset managers and banks are piloting tokenized funds, on chain settlement, and partnerships with public chain infrastructure. For IT teams, this introduces questions around governance, custody integration, data lineage, identity management, and regulatory reporting. Early deployments are often focused on collateral management or private market funds, where tokenization simplifies settlement and reduces operational friction.

While the regulatory landscape continues to evolve, the pace of experimentation within institutions has accelerated. IT leaders are being asked to support these initiatives with secure, compliant environments capable of integrating with blockchain networks without introducing risk to core systems.

***On-chain finance is moving from concept to implementation.***

*IT leaders must prepare for governance, custody, integration, and data-lineage challenges associated with digital asset pilots.*



## INCREASING DATA AND ANALYTICS REQUIREMENTS DRIVEN BY CAPITAL AND MARKET RISK RULES

Changes in capital requirements and market risk calculations are placing new demands on data quality, granularity, lineage, and model validation. Institutions are enhancing their analytics infrastructure to support complex risk engines and new reporting requirements. This includes scaling compute resources through hybrid cloud models, improving the accuracy and traceability of data used for regulatory submissions, and automating reporting pipelines to reduce manual processes.

This type of modernization is not optional. Risk and finance teams are relying on IT to deliver infrastructure that supports more complex models, faster iteration cycles, and more rigorous validation and audit processes.

***Risk regulations are tightening data expectations.***

*Stronger data quality, lineage, and analytics are now essential for meeting capital and market risk requirements.*



## CLOUD AND DATA MODERNIZATION UNDER COST AND COMPLIANCE PRESSURE

While cloud adoption continues to expand in financial services, the strategy behind it has matured. Accenture research shows that although 82% of financial leaders view hybrid cloud as essential for transformation, fewer than half feel fully mature in their cloud execution. Institutions are moving away from broad lift and shift strategies toward more targeted modernization that balances agility, performance, sovereignty, and cost control.

This means strengthening data foundations, consolidating legacy environments, improving lineage and access controls, and selectively migrating workloads that benefit from elasticity or adjacency to AI. Many organizations are also replatforming legacy applications to reduce technical debt and improve resilience, while maintaining sensitive workloads on premises or at the branch edge.

**Hybrid cloud maturity is still low, even as demand rises.**

*Although 82% of financial executives agree that hybrid cloud is essential, fewer than half feel mature in their implementations. Modernizing data foundations is critical.*



## MODERN BRANCH AND EDGE IT TO SUPPORT BOTH UPTIME AND INNOVATION

Even as digital adoption increases, branches remain essential for relationship driven banking and regulated services. Yet many branch environments run on aging hardware, inconsistent networking, or manual patching processes that create operational risk.

Modern branch and edge infrastructure helps institutions centralize management, reduce downtime, and deploy updates more consistently. Running teller systems, ATM applications, and compliance related workloads locally improves resilience during WAN disruptions, while cloud based management reduces the cost and complexity of supporting distributed environments. This modernization directly impacts customer experience, particularly in regions where physical locations remain an important channel.

**Branches remain operationally important and must be modernized.**

*Edge platforms, centralized management, and consistent security controls help improve uptime and reduce operational cost.*



## ZERO TRUST SECURITY FOR HYBRID WORK AND EXPANDING THIRD PARTY ECOSYSTEMS

With hybrid work now a permanent fixture and third party fintech integrations growing rapidly, traditional perimeter-based security is no longer effective. IT teams are implementing Zero Trust architectures with continuous identity verification, least privilege access, and stronger device and network posture checks. These controls help reduce exposure to ransomware, insider threats, and credential-based attacks, which remain among the most common entry points in the financial sector.

Regulators and insurers increasingly view Zero Trust as a standard expectation, not an advanced practice, and many institutions are prioritizing its implementation across data centers, clouds, and branch locations.

**Zero Trust is becoming the new baseline.**

*Continuous verification, least privilege access, and device posture checks are now required to maintain security across hybrid work and legacy ecosystems.*



## TALENT SHORTAGES AND LEGACY COMPLEXITY MAKE MANAGED SERVICES STRATEGIC

Financial IT environments continue to grow in complexity, yet the availability of specialized talent in areas such as cybersecurity, cloud architecture, and regulatory compliance remains limited. Deloitte surveys show that a majority of financial services CIOs report difficulty hiring and retaining skilled professionals who can support modernization efforts.

As a result, many organizations are turning to managed services to stabilize operations and focus internal talent on high value initiatives. Managed services help institutions maintain consistent patching, monitoring, and incident response, support structured migration and modernization efforts, and scale securely without expanding internal headcount. This model also creates predictable operational costs and reduces the burden of maintaining highly specialized skill sets in house.

*Managed services fill critical skills gaps as expertise growth scarce.*

*With more than half of CIOs struggling to hire skilled specialists, managed services provide stability, resilience, and the ability to accelerate modernization without expanding headcount.*

### CASE STUDY

## LEADING INSURER MODERNIZES 22-YEAR-OLD JIRA ENVIRONMENT WITH MANAGED MIGRATION EXPERTISE

A top 10 global property and casualty insurer partnered with Verinext's Forty8Fifty Labs to modernize its 22-year-old Atlassian Jira environment—used daily by over 20,000 users and 8,500 agents. The legacy system had undergone 14 upgrades and required a carefully orchestrated migration to Jira Cloud.

Forty8Fifty Labs conducted a two-month assessment and developed a tailored migration strategy, successfully executing the transition through three test passes and final cleanup. The result: a fully modernized cloud-based environment optimized for scale, with strong validation from third-party reviewers.

[READ THE FULL STORY](#)



## MODERNIZING FINANCIAL IT FOR A MORE RESILIENT AND INNOVATIVE FUTURE

If you're leading IT inside a financial institution, you are facing one of the most challenging transitions the industry has seen. You are being asked to support AI initiatives, strengthen cyber defenses, prepare for instant payments, explore tokenization pilots, and keep pace with shifting regulatory expectations, all while maintaining seamless experiences across digital channels and branch environments.

You do not need broad predictions about the future. You need an IT foundation that helps you handle today's demands with confidence. By advancing your hybrid cloud strategy, strengthening data governance, modernizing branch and edge environments, adopting Zero Trust security, and leaning on managed services where specialized expertise is scarce, you can reduce risk, improve operational efficiency, and create space for innovation. Most importantly, you can give your organization the resilience it needs to serve customers securely and reliably, no matter what comes next.

**Verinext provides the expertise and services that help financial IT teams modernize with confidence and maintain the resilience, security, and compliance required across highly regulated environments.**

**To explore your modernization priorities and next steps, contact Verinext or review our Financial Services IT Modernization Infographic [here](#).**