

5 signs your infrastructure is holding you back

Simplify IT and Safeguard Your Accountholders

One of the biggest barriers to cloud modernization isn't budget. It's uncertainty.

How will you manage greater complexity? Can you strengthen security without overburdening your team? Will a new model satisfy regulators? And can you modernize without disrupting your financial institution's daily operations or your accountholders' daily lives?

Those are valid questions. But staying on-premises carries risks of its own as technology advances, regulatory expectations evolve, and accountholders expect faster, more seamless experiences.

Advancements in artificial intelligence have fundamentally changed the speed and scale of cyberattacks. Adversaries are now utilizing frontier AI models to identify, prioritize, and chain together software vulnerabilities at machine speed. As cyber threats continue to evolve, financial institutions need security architectures capable of detecting, predicting, and responding just as quickly.

1. Capital Efficiency

Maintaining aging infrastructure can consume resources that could otherwise support strategic priorities.

Hardware refreshes also introduce procurement, business continuity, and disaster recovery considerations, while specialized audit, automation, and monitoring requirements



can place additional demands on internal teams.

Moving from a traditional capital expenditure model to a cloud operating expenditure model gives you another option.

With Jack Henry® Managed Secure Cloud for Microsoft Azure (MSC-Azure), a part of the Gladiator® Suite of Services, you can replace hardware investments with a consumption-based model designed to make costs more transparent and predictable. Pricing is based on consumption rather than users or assets, helping the model scale with your needs.

2. IT Capacity and Control

Your technology team shouldn't have to choose between keeping infrastructure running and moving your financial institution forward.

Legacy environments can keep skilled employees focused on maintenance, patching, monitoring, and infrastructure management. Building all the expertise and tooling required to manage a modern environment internally can also add cost and complexity.

MSC-Azure provides a co-managed alternative. Jack Henry manages areas such as security, maintenance, and monitoring while your financial institution retains oversight of its dedicated Azure tenant. This can help free your team to focus more attention on modernization and the technology initiatives that differentiate your financial institution.

And because Managed Secure Cloud is core and device agnostic, your cloud strategy doesn't have to depend on a specific core or endpoint environment.

3. Information Security and Business Resilience

The question isn't simply whether cloud infrastructure is secure.

It's whether your operating model can continuously manage changing threats, vulnerabilities, outages, and recovery requirements. Advances in frontier AI models have



Modernization isn't simply an IT expense. It's an opportunity to redirect resources toward higher-value priorities.

fundamentally changed the speed, scale, and sophistication of cyberattacks. Adversaries can now identify, prioritize, and chain together vulnerabilities at machine speed, compressing the time between discovery and exploitation. Defending against these emerging threats requires security operations that combine predictive intelligence, automation, Zero Trust principles, and continuous monitoring.

MSC-Azure brings multiple safeguards together, including infrastructure-as-code, drift control, Azure Policy guardrails, role-based access control, SASE security, endpoint detection and response, 24/7 monitoring and response, and SIEM capabilities. Through the Gladiator® Suite of Services, Jack Henry helps financial institutions defend against machine-speed attacks with AI-powered predictive defenses, automated response playbooks, Zero Trust architecture, and 24/7/365 monitoring and response delivered through the dedicated Gladiator Security Operations Center (SOC).

Resilience extends beyond cyber defense.

Dual-region failover and immutable, air-gapped backups are designed to help maintain operations and accelerate recovery from ransomware, natural disasters, technology failures, and cloud outages. This integrated approach can reduce the burden of assembling and managing separate security and resilience solutions yourself.

4. Growth and Innovation

Infrastructure decisions can either accelerate your growth strategies or introduce friction at every step.

Modern cloud architecture can give you a stronger foundation for initiatives such as digital onboarding, lending, mergers and acquisitions, faster payments, APIs, and fintech integrations. Instead of working around infrastructure constraints and data silos, you can focus on delivering new capabilities and connected experiences.

MSC-Azure is designed to provide the secure, governed



Resilience isn't just about preventing disruption. It's about knowing how quickly and confidently you can recover when disruption occurs.

foundation those strategies require, helping you reduce technical debt and create an environment that can support evolving applications, data, automation, and AI.

As organizations adopt AI-enabled applications and automation, they must also contend with threats powered by frontier AI models that can accelerate reconnaissance, vulnerability discovery, and attack execution. A secure modernization strategy requires infrastructure designed not only to support AI innovation, but also to defend against increasingly sophisticated AI-driven attack techniques.

The result is not innovation for innovation's sake. It's greater flexibility to respond when your financial institution, market, or accountholders demand something new.

5. Regulatory Confidence and Operational Oversight

Adding more technology can sometimes mean adding more vendors, assessments, evidence collection, and administrative work.

A more integrated model can simplify that equation. Managed Secure Cloud brings critical capabilities such as firewall, backup, cloud hosting, compliance software, endpoint protection, and monitoring into a more cohesive environment. Governance, Risk, and Compliance capabilities further help you manage asset inventory, governance policies, reporting, and oversight.

You can maintain visibility through dashboards, compliance reports, scheduled custom reports, monthly service reviews, and integrated GRC management while drawing on Jack Henry's dedicated governance, risk, and compliance expertise.

That combination matters when you're weighing your options: you don't have to approach modernization as a choice between greater flexibility and greater control.



Your infrastructure should be an enabler of your growth strategy, not another obstacle your strategy has to overcome.

support for the cloud model that fits your financial institution

Cloud modernization doesn't have to mean taking the same path as every other financial institution.

Jack Henry Managed Secure Cloud supports private, public, hybrid, and multi-cloud environments, giving you options to balance efficiency, security, resilience, compliance, and control according to your needs.

And you don't have to navigate those decisions alone. Jack Henry brings years of experience as a technology adviser, dedicated governance, risk, and compliance expertise, strong integration, and industry-focused support.



The goal isn't to move compliance somewhere else. It's to make compliance and oversight easier to manage.

modernize securely and confidently

Discover how [Jack Henry® Managed Secure Cloud](#), delivered through the Gladiator® Suite of Services, can help you balance modernization with control, security, resilience, and operational oversight as part of your broader cloud strategy.

For more information about Jack Henry, visit jackhenry.com.