Fieldwork

How regulated industries can make IT modernization work - on their terms

Even the most closely regulated organizations can make transformative upgrades that prepare them for tomorrow.

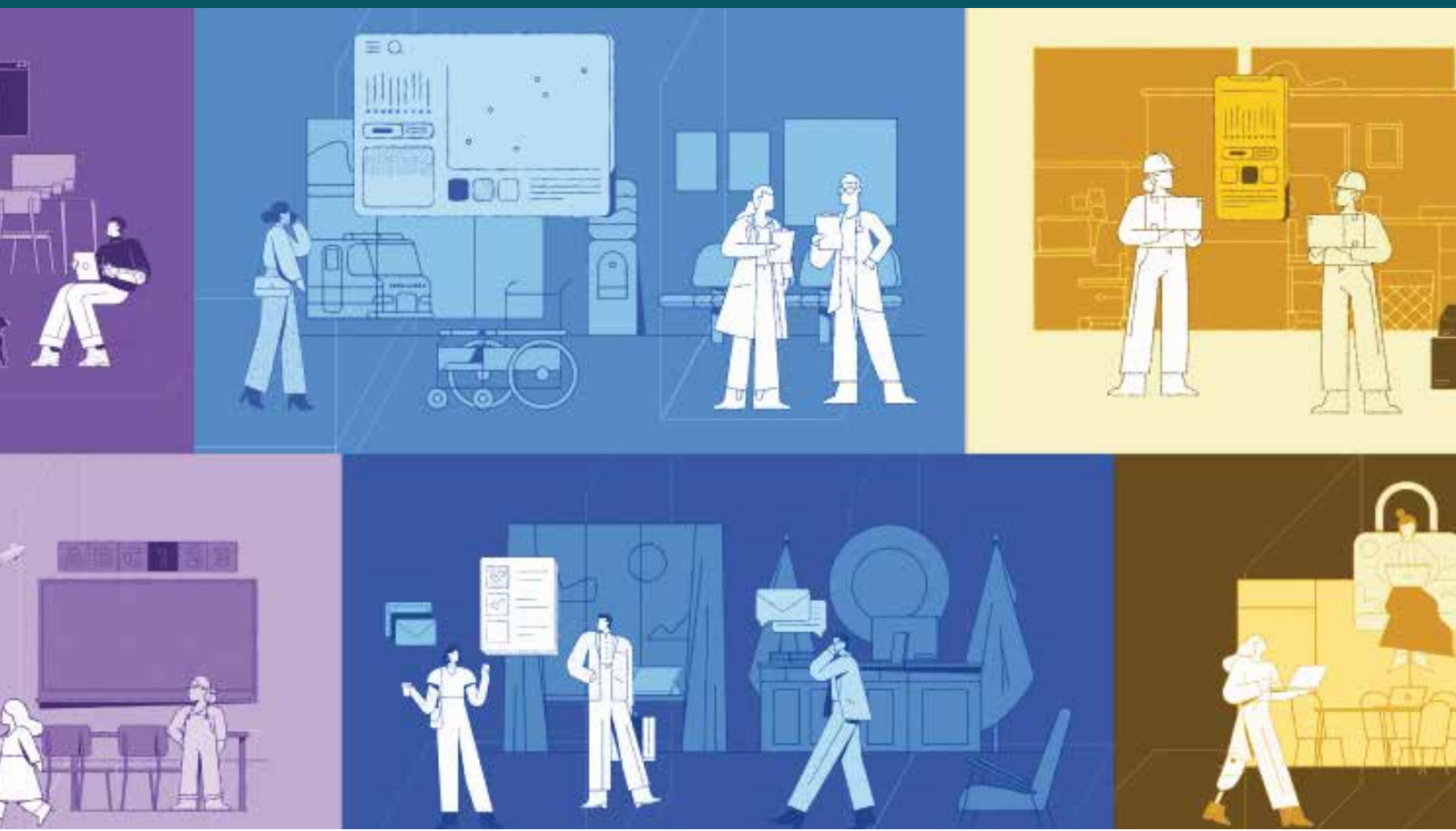

Table of contents

Many businesses transforming their IT operations talk a big game. If you sell or manufacture widgets for everyday consumers, it's easy to shout about your cloud migration successes, how you've empowered your people to work from anywhere, and what your 2025 IT modernization roadmap looks like. But organizations in regulated industries — particularly finance, healthcare, insurance, as well as agencies and vendors in state and local government and education (SLED)
— operate by a different rulebook.

For these organizations, the path to IT modernization is anything but simple. Regulatory and compliance needs can often limit their IT solution and infrastructure flexibility.

Granted, businesses and agencies charged with safeguarding financial markets, patient data, tax records, and public welfare should be held to a higher standard than an e-commerce platform selling artisanal cheese. But with great responsibility comes great challenges, whether in IT provisioning, systems integration, or end-user experience delivery.

All this can make IT modernization feel too difficult, too expensive, too overwhelming. It's why many organizations choose to double down on existing models rather than preparing for a dynamic tomorrow.

But make no mistake, IT modernization is not just an ambition, but a precondition of success in today's world of work. Organizations that aren't evolving their IT strategies will face new, more daunting challenges tomorrow. In fact, the has accelerated the widespread shift to hybrid work need to adapt, and even organizations in heavily regulated sectors are taking steps to become more agile and modernize at a pace that's right for their team and industry. They understand that a project of this size isn't a "one and done." Implementation can occur incrementally, where pieces are added or retired based on the organization's needs and priorities.

Here are some key considerations and strategies that organizations in regulated industries can adopt into their IT practice.

Right-pacing IT modernization

The savviest teams in regulated industries prioritize solutions that not only fit the moment, but create the flexibility to evolve and add sophistication over time.

Many organizations are of hybrid on-prem/cloud models. Such models help ensure weighing the merits regulatory compliance by keeping sensitive data in the organization's real estate footprint, while allowing teams to implement cloud-based software and management solutions quickly and efficiently, ensuring secure access from virtually anywhere. This can also be cost-effective, as it breaks the cycle of upgrading expensive server equipment every five years.

The thought of moving to the cloud can intimidate even the most forward-thinking IT leaders. But it shouldn't. "We used to hear from our clients, It's cloud, we're regulated, we don't put data there,'" Damien Bartlett, Insurance Sector Lead, Citrix, says. "And yet they were already using Microsoft 365 or SaaS cloud services." Organizations using cloud-based enterprise software platforms have already taken meaningful steps toward IT modernization. Acknowledging that can take some trepidation out of the equation.

The key is to start small, with a symbolically important step. For example, locating your business continuity and disaster recovery (BCDR) plan in the cloud allows an organization to achieve important security redundancy and send a clear signal of your intent to house operations and deploy increasingly via the cloud.

As upgrade cycles are plotted, organizations can continue moving more "pieces" of their tech to the cloud. An intelligent IT modernization strategy allows businesses and agencies to transition gradually, building increased flexibility while maintaining control and data security. (Of course, It's also possible to migrate in one go. The Financial Industry Regulatory Agency, better known as FINRA, moved from on prem to the cloud, and hasn't looked back.)

“

Even people who want to go full cloud don't want to do it tomorrow. But at their own pace, they can identify the use cases, understand how to deploy what to whom, and maintain cost control while ensuring the flexibility to scale the number of users they need.

Christian Boucher
Chief Healthcare Strategist, Citrix

Increasing data security in insecure environments

With many employees in regulated industries sitting beyond the traditional firewall, it's more important than ever to ensure secure access to information, wherever people do their jobs. A doctor reviewing a patient's chart on their backyard patio; a trader messaging from her wearable; a professor accessing research in the field — they all depend on their employers maintaining a "never trust, always verify" posture, without losing sight of the importance of simplicity and ease of use.

"Security has to be at the very top of the list when you architect," says Terry Aoki, EVP and CDO at Right! Systems, an IT consultancy based in the U.S. Pacific Northwest. "If it's not, then you're the next person we're going to read about in the news.

The goal of any IT modernization project should be to protect all users, apps, and data without creating silos or disruptions. "How do you get the same good experience for every single one of those users? You have to build something that is consistent," Aoki says.

An organization's security approach must shift from unconditional confidence in users to zero trust fundamentals. For example, securing managed and unmanaged devices by scrambling keystrokes and returning screenshots as blank screens can mitigate the risk from bots catching on. Zero trust network access (ZTNA) also helps drive productivity for remote users and mitigates security risks.

Adaptive security becomes important, too. What happens when an employee travels to a conference and needs to access information, but is out of the approved geographical area? What about a bank representative who is approving mortgage contracts via a tablet, only to have the tablet stolen? Taking a generous view of the potential risks, and implementing IT solutions accordingly, helps data stay safe, no matter how remote the edge case.

“

With Bring-Your-Own-Device [BYOD] ... there's a technical wrapper of device, access, and security. Things like ZTNA, as well as anti-screen scraping and anti-keylogging , are especially effective with BYO because bots can't lift or capture the data.

Damien Bartlett
Insurance Sector Lead, Citrix

Scaling a modern workforce quickly and efficiently

In addition to securing data, IT modernization can enable organizations to scale quickly and effectively in a variety of scenarios. This is especially important in regulated industries like healthcare, where consolidation activity is happening at a rapid pace. Whether to onboard new team members or create security clearance tiers, flexible systems should be in place before the merger champagne is popped.

These IT innovations also help prevent a "two-tiered" workforce from emerging by helping counter proximity bias. "You can ensure employees can work and not encounter bias, whether they choose to be in office or at home," Bartlett says. "This applies both to new hires who prize WFH and established staffers who are accustomed to the office environment and may want to be there."

Effective IT modernization also frees organizations to scale software as needed for specific employees. Desktop as a service, or DaaS, allows employees to consume applications on demand, which provides flexibility and helps control costs. One employee might only need access to a single application, whereas a power user might need an entire virtual setup. IT teams can identify how to deploy what to whom.

"Think about a medical office," Christian Boucher, Chief Healthcare Strategist, Citrix, says. "You might have five doctors who want to work one way, five who want to work another, and five who want a combination." With DaaS, IT leaders have pinpoint control over each doctor's experience, and can tailor and deploy accordingly.

“

Imagine you’re moving an organization with 20,000 employees from one enterprise collaboration platform to another. It’s difficult to adhere to a security department’s authentication requirements if proper processes are not established first.

Chad Price

Practice Manager, Infrastructure Platforms, Burwood Group

Preserve Cloud Service Provider flexibility while maintaining security

The fear of being locked into onerous, restrictive cloud service provider (CSP) agreements may contribute to regulated organizations' skepticism around IT modernization. IT leaders are rightfully wary of signing budget-sapping contracts with one cloud provider. Meanwhile, relying on one CSP's security systems could make it difficult to change later. The right cloud services provider, however, can update at a layer removed from the cloud platform — and agnostic of the cloud chosen — to maintain enterprise flexibility.

This is the best of both worlds: the ability to pick and choose the right services and security today, and well into the future. Organizations can preserve their existing relationships with service providers, whether it's Microsoft, Google, AWS, or a combination of partners, and build a hyper-secure layer over the top.

"It's not about locking teams into any one schedule or offering," Boucher says. "The focus should be on allowing a company to adopt any solution, on any platform, as they deem necessary." And since the newest IT modernization features will deploy cloud-first, it makes sense for organizations to focus their modernization and security efforts at that level above the CSP.

Working from that remove can also help prevent "cloud sprawl," which is valuable particularly among SLEDs, where budgets tend to be more constrained. But the bigger unlock is a fundamental reframe of enterprise security. No longer is data security a siloed activity in your organization or a cost center in your budget, but a wrapper that envelops your workspace technology, regardless of cloud platform.

“

If you’re in these regulated industries like healthcare, banking, and government, and you have to take whatever security that the cloud platform builds into their systems — and then you learn the csp doesn't work for you — it's really hard to make a change.

Terry Aoki

EVP and CDO, Right! Systems

The new world of work requires IT modernization

Work has moved from on-prem to everywhere, and executives and IT leaders must adjust their data security practices accordingly. Simply put, IT modernization is critical for success in today's world of work. The tools for effecting real change — whether it's DaaS, ZNTA, SSO, or others — are available now, and there's never been a better time to start leveraging them.

"For IT professionals, IT modernization boils down to a mindset shift: If you're in IT, your job is no longer equipment, it is experience," Aoki says. That means that as the security edge extends, IT teams should embrace tech that protects data without degrading the employee's experience or a customer's interactions.

This is a monumental reimagining of the role of IT. But it is also a tremendous opportunity. "As technology continues to evolve, the IT team remains enormously valuable to your business," Chad Price, Practice Manager, Infrastructure Platforms at Burwood Group, says. "An IT systems engineer might become a business analyst in app modernization. After all, nobody knows their systems and apps better than them."

IT teams are core to IT modernization. This may be the most compelling reason to do this vital work. By bringing the right tools and platforms into the organization, IT leaders empower their people to become agents of progress — not just for the organization, but in their own careers.

citrix

Enterprise Sales
North America | 800-424-8749
Worldwide | +1 408-790-8000

Locations
Corporate Headquarters | 851 Cypress Creek Road, Fort Lauderdale, FL 33309, United States
Silicon Valley | 4988 Great America Parkway, Santa Clara, CA 95054, United States