Impact Study | In association with: Tanium

The CIO’s guide to architecture modernisation through portability, resilience, and flexibility

June 2022

Finextra | TANIUM

Contents

01 | Introduction: Why CIOs need to shelve short-termism in favour of smart modernisation

Every architecture decision a CIO makes directly impacts their bank's competitiveness and success. This is truer than ever as competition and disruption from agile, fast-moving players continues to increase and they scoop up customers who are eager to interact in new ways with their financial services providers.

The infrastructures on which the traditional financial services industry — and banks in particular — have been built aren't holding up to this pressure. Their response? Single-threaded point solutions, and lots of them.

However, these aren't solving problems for the long-term — or, arguably, even in the short-term. Rather, they're exacerbating a growing architectural issue, adding to the inefficiency and lack of scalability of their IT environments. They're also making it harder to get a clear, unified view of the whole estate. Instead, banks continue to accumulate technical debt, create integration headaches on a colossal scale, and ultimately fail to rise to the challenge that today's financial services ecosystem demands.

Of course, banks have legacy infrastructure to consider. Abandoning these investments isn't an option. But building alongside them using cloud and new technology is. Banks need to consider how to bring together the operational domains of customer, application, infrastructure, and security. Through modernisation and automation — and combining the best of existing and new – they'll be able to connect data silos, integrate systems, and enable real-time visibility to deliver improved services faster and more securely.

The bottom line is, banks' CIOs need to do more than merely resource the next project. They should be working towards increased visibility on all levels to provide long-term resilience for their organisations and most importantly, their customers. And whether success means enabling their global workforces to work from home today, tomorrow, or next year — or upping the game when it comes to customer interactions — they'll be able to do that, and more, underpinned by a modern infrastructure.

02 | Getting a grip on the edge: the importance of portability, resilience, and flexibility

The complexity of managing dated and often brittle architectures, especially for established institutions with decades' worth of legacy infrastructure investment, is a persistent and growing concern for CIOs. On top of rapidly ageing and expensive core systems, there's an expanding raft of cloud-based tech alongside a proliferation of devices that all need to work together seamlessly and securely.

Debt, noise, and confusion

The key issue with legacy architecture is that while financial institutions have dipped their toes into modern technology — particularly cloud — the fact that they're now working with a plethora of environments means they can't grab the edge anymore. Successive years of investments into technology have resulted in heavy technical debt accumulation and confusion as to where in the network builds are actually occurring.

A survey of financial services and tech leaders by **McKinsey** shows that CIOs estimate tech debt to account for 20–40% of the value of their entire IT estate. Point solutions have been amplifying the noise and complexity rather than addressing any of the big challenges banks face. These include combatting security threats, enabling flexible and remote working en masse, and delivering improved services to customers.

By continuing to develop and deploy new features in the same manner that they've always done, banks are getting further from the solution with every new release and are making investments that only throw off short term value impact for the firm. Further from architectural resilience. From portability of workloads, apps, and data. And from operational, infrastructure, and service flexibility.

Trust no one

Cybersecurity is central to any discussion of the challenges around infrastructure modernisation, especially when it comes to organisations that require the highest levels of security due to being exposed to some of the highest levels of risk.

With every new device or development within the IT environment, banks' attack surfaces broaden. So given the rate of change even before the pandemic, keeping ahead of evolving threats is a significant ongoing challenge for CIOs.

For instance, in today's landscape, zero trust is an accepted and necessary approach to cybersecurity for financial services organisations, which are in the front line of potential attack. But how does a bank go about developing and implementing an effective zero trust strategy? There are many different and equally valid approaches under the zero trust umbrella, but putting the right controls and practices — from detecting anomalous behaviour to setting up least privilege access policies — is a minefield in itself. This is aside from the fundamental issue that banks are often reluctant to adapt their working architectures (in any direction) because of their typically risk- and change-averse natures.

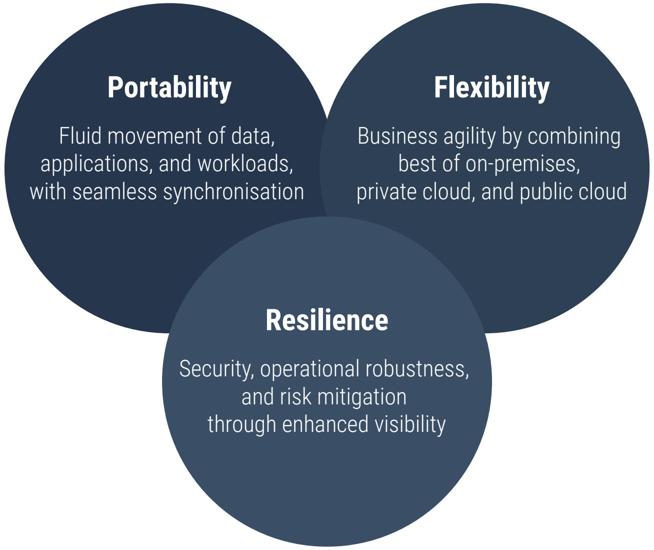
The simple answer is, it's not easy. And banks have it hardest in large part because their infrastructures are so disparate, have evolved over so many years, and are so difficult to get a clear view of.

All roads lead back to knowing each component, and the points of their interconnection, across your entire architecture — clear visibility and line of sight to all services, devices, users, data.

The path to portability, resilience, and flexibility

For CIOs, working towards higher degrees of portability, resilience, and flexibility is the key to bringing the infrastructure together, creating a secure environment end-to-end, and being able to view and understand all of its components. These interconnected concepts lie at the heart of banks' transformations.

Figure 1: Three pillars of architecture transformation



Portability

Fluid movement of data, applications, and workloads, with seamless synchronisation

Flexibility

Business agility by combining best of on-premises, private cloud, and public cloud

Resilience

Security, operational robustness, and risk mitigation through enhanced visibility

With data and apps running on different on-premises and cloud-based platforms, being able to move infrastructure and application workloads automatically and seamlessly without disrupting business as usual — as well as synchronising data as required — is a critical feature of modern infrastructure.

This ability to transfer workloads, scale as necessary, and get the best value and performance from each environment is how banks become agile. And also how they achieve operational robustness, increased security, and more effective risk mitigation.

In a **Tanium** survey of financial services IT leaders, 91% admitted to weak points on the network causing visibility gaps and 52% said that each week they identified endpoints within the organisation of which they were previously unaware. The priority for banks' CIOs is to gain full visibility of the ever-shifting edges of their networks. Understanding where those edges are, where their network sits, and where data is being produced, held, and encrypted. Not just in what cloud or on what server – but across containers, laptops, microservices and the growing number of endpoint devices. And, what's more, not just knowing what data they're handling, but ensuring that data's protected, works with the larger organisation's infrastructure, and can be accessed and moved to different environments and devices as required to maximise performance.

This, in a nutshell, is the starting point on the road to resilience.

03 | Data, everywhere…

While data is all around, its usefulness is minimal unless we have control of it. More than that, it's a liability if we don't handle it correctly and with care. On a basic level, it has to be secure and transparent. Which means you need to know where it is, where it's going, and who's doing what to it.

The cost of cyberattacks to financial institutions continues to grow — with the average price tag of a data breach in the financial sector coming in at $5.72 million, according to **IBM**. But the reputational damage that data in the wrong hands can cause is arguably worse. Endpoints are where the greatest opportunities and the greatest risks lie. For a big bank, we're talking about hundreds of thousands if not millions of endpoints across geographies. And the more endpoints, tools, and technology you have, the more your data is a risk rather than a competitive advantage. That financial services firms are 300 times more likely to be vulnerable to cyberthreats than other companies isn't surprising, as highlighted by the Boston Consulting Group.

The best approach for CIOs to take to address the challenges of the all-too-familiar endpoint sprawl is a continuous cycle of rationalising, reviewing, and integrating.

- **Know what you know — and what you don't**
  What's the current landscape? How has the legacy mentality of buying two of everything impacted where you are today? CIOs must start by rationalising all of this and understanding the policies that have created the infrastructure as it stands. They must also understand that rationalisation of portability and ease of integration of the estate components is critical.

- **Get your data house in order**
  Banks need to make sense of and get clarity around the data that's being produced at device level. By streamlining tooling, processes, and technology, CIOs put themselves in a better position to understand the data that's floating around in apps, on devices, and across platforms. This can then be used to not only identify where weaknesses are, but also improve services and create new experiences for customers.

- **Make your risk profile a priority**
  Once you have a clear view of the IT estate, CIOs can start to build a more strategic approach to risk. This involves evaluating your risk profile from all angles — assets, cloud-based services, devices, and networks — to create a portability index that assesses the risk of every infrastructure move.

- **Bring security management and IT ops together at the table**
  This is the crux of the whole process, and the first major step in the journey towards automation. Converging capabilities and simplifying infrastructure through integration starts with finding a common language between security management and IT operations. Between them, they need to consolidate the many control panels that accompany disparate legacy architectures and cause failures of communication.

With a consolidated view and single source of truth around endpoint telemetry, there's a better likelihood of understanding where data is and how it's being used. Which means a better chance of orchestrating that data from different sources across the organisation on fewer control planes to create real value to the bank and its customers. Moving from manual orchestration of data to an automated delivery model is critical to reducing a bank's attack surface and overall risk profile.

04 | Opportunity and risk in the cloud

With so much focus on architecture modernisation, it's easy to get the impression that legacy technology is merely a hindrance. But while the cracks are showing in existing architecture, it's still an essential part of banking's core. Equally, there's no way banks can afford not to modernise. And they need to do more than just dabble with cloud services and new technology.

The challenges for CIOs are threefold:

- There needs to be a shift of workloads to more appropriate cloud-based platforms
- On-premises and cloud infrastructures must be made to work fluidly together
- The growing number of endpoints and expanding edge connections require a greater degree of visibility

Engage cloud to compete

Cloud can complement existing infrastructures, adding the benefits of scale, cost-efficiency, and flexibility. With automated processes, the capacity for banks to innovate and compete with newer entrants becomes possible. It's an environment in which success is no longer measured by availability and uptime, where we used to add zeros to the cost for every additional 9 of availability — a massively cost prohibitive model. Success is now all about latency, error rates, response times, vulnerability metrics, and — crucially — user experience.

Cloud usage is being driven by the need for banks to not just continue growing revenue and core customer relationships exponentially, but also maintain overall business health. The move has generally been slow, but is gathering pace. **EY** reported that UK banks had moved just 10% of their business infrastructures to the cloud, but 27% expected to migrate at least half of their apps and/or systems by 2022.

In terms of scaling the business, cloud allows banks to find new customers and white space, or even expand their customer lifecycle into new spaces, in a cost-effective manner. It's also what enables new self-service delivery models, enabling banks to reach many more potential customers and acquire them quickly and safely. Once onboarded, these customers expect the highest level of performance and experience, so the technology needs to work seamlessly. This is where making sure the connections between all parts of the infrastructure are robust and secure – and why visibility is the CIO's most valuable weapon.

Shift and de-risk

A common approach to using cloud alongside on-premises architecture involves developing front-end services in the cloud and plugging in to what's generally an old and often brittle back end. The challenge isn't merely making these two systems work together, but making sure you don't sacrifice security in the pursuit of competition.

The threat is often misinterpreted. That the cloud part is in the cloud isn't the point. It's the huge number of additional connections it creates that must be protected as these often create new doors for attackers to come through and reach core systems. Therefore banks must now consider that there are a greater number of threats, a greater number of potential attacks, and a greater number of vulnerabilities — often happening in plain sight.

Bad actors don't generally care how they access the data and systems they want to get hold of or into. And they'll exploit any visibility gaps that occur, especially where there's limited internal knowledge of network end points and the perimeter is wobbly at best.

The good news is, creating a hybrid cloud environment can help de-risk platforms. The security profile in the cloud, by design, is far more sophisticated because it was architected to be multi-tenant from a user and data perspective. Also,

because security is a top priority cloud providers spend a much larger percent of their budgets in this space than most banks can afford as most of the investment continues around the care and feeding of the legacy. The importance of visibility in this complex landscape is obvious. Banks need an accurate picture at all times across all devices and data. Out-of-date information on IT operations and security is useless. Likewise, tools that tell you only part of the story or report data in one area of the business or on one platform.

For CIOs, an agnostic approach is required, backed up by data-driven decisions to responsibly move workloads to the cloud.

05 | Focusing on the experience

Cloud is key to customer experiences. Banks are competing with a range of financial and fintech players that are cloud-native (as well as, increasingly, non-financial organisations that are now embedding financial services). With no legacy infrastructure, new entrants on the financial services scene can create integrated, agile environments from the ground-up — an advantage traditional financial institutions don't have. So, as we've seen, they need to work harder at bringing everything together.

360-degree visibility

Many banks are still operating core customer interactions on legacy infrastructure, which is why patching up and applying point solutions continues to be the norm. And why it feels easier to continue to pay the interest on technical debt.

With modernisation, the tech transformation is simple in comparison to retaining customers under the realm of new services. This is the most significant part of any change that's implemented: there's a dichotomy between the need and drive towards digitalisation, and the reality of banks and their customers being able to keep pace.

To modernise and provide self-service models. To enable fast onboarding and access to innovative applications and services. To make decisions driven by real-time data. All of this requires a transformation of how CIOs manage and monitor their ever-growing estates that include a multitude of endpoints and platforms, including laptops, mobile devices, servers, containers, and multiple cloud services. The customer experience is the ultimate goal: where the benefits of automation, portability, and flexibility of infrastructure come together.

By investing in the processes, technology, and policies that enable these architecture qualities, CIOs are directly investing in the services their banks can deliver to customers.

06 | Conclusion: From technical debt to automation

Architecture modernisation and the confluence of customers, applications, infrastructure, and security is the only route to relevant transformation for banks. Working with on-premises and multi-cloud environments, banks' CIOs must architect in the direction of portability, resilience, and flexibility. So that all elements connect seamlessly, all workloads move dynamically, and all endpoints are seen as well as protected at all times, and in real or near real time.

For banks' CIOs, any architecture modernisations programme should be driven by three strategic goals:

1. Find the gaps. Know your strong and weak points by prioritising visibility across your whole IT estate.
2. Stop the bloat. End the negative cycle of rolling out point solutions and put your banks' money where the smart technology is…in integrated platforms.
3. Bring everyone together. Or, more specifically, IT ops and security management. This is probably your most crucial step and the one that's most critical to achieving data transparency and automation.

By making progress in these areas, banks will be able to gain a larger slice of the market opportunity in the face growing competition.

About

Finextra Research

This report is published by Finextra Research.

Finextra Research is the world's leading specialist financial technology news and information source. It offers more than 130,000 fintech news, features and TV content items to some 800,000 monthly visitors to www.finextra.com.

Finextra covers all aspects of financial technology innovation involving banks, institutions and vendor organisations within the wholesale and retail banking, payments and cards sectors worldwide. Finextra's unique member community consists of over 40,000 fintech professionals and 200,000 social followers working inside banks and financial institutions, specialist fintechs, consulting organisations and technology providers.

The Finextra community actively participates in contributing opinions, ideas and comments on the evolution of fintech.

For more information:

Visit **www.finextra.com** and become a member,
follow **@finextra** or reach us via **contact@finextra.com**.

Tanium

Tanium, the industry's only provider of converged endpoint management (XEM), leads the paradigm shift in legacy approaches to managing complex security and technology environments. Only Tanium protects every team, endpoint, and workflow from cyber threats by integrating IT, Operations, Security, and Risk into a single platform that delivers comprehensive visibility across devices, a unified set of controls, and a common taxonomy for a single shared purpose: to protect critical information and infrastructure at scale.

Tanium has been named to the Forbes Cloud 100 list for six consecutive years and ranks on Fortune's list of the Best Large Workplaces in Technology. In fact, more than half of the Fortune 100 and the U.S. armed forces trust Tanium to protect people; defend data; secure systems; and see and control every endpoint, team, and workflow everywhere. That's the power of certainty.

Visit us at www.tanium.com and follow us on LinkedIn and Twitter.

For more information

Finextra Research
77 Shaftesbury Avenue
London,
W1D 5DU
United Kingdom

Telephone
+44 (0)20 3100 3670

Email
contact@finextra.com

Follow
@finextra

Web
www.finextra.com