Converge™
by Deloitte

Building the foundation of a future-focused bank

IT architecture from Deloitte and AWS addresses industry-specific challenges

aws

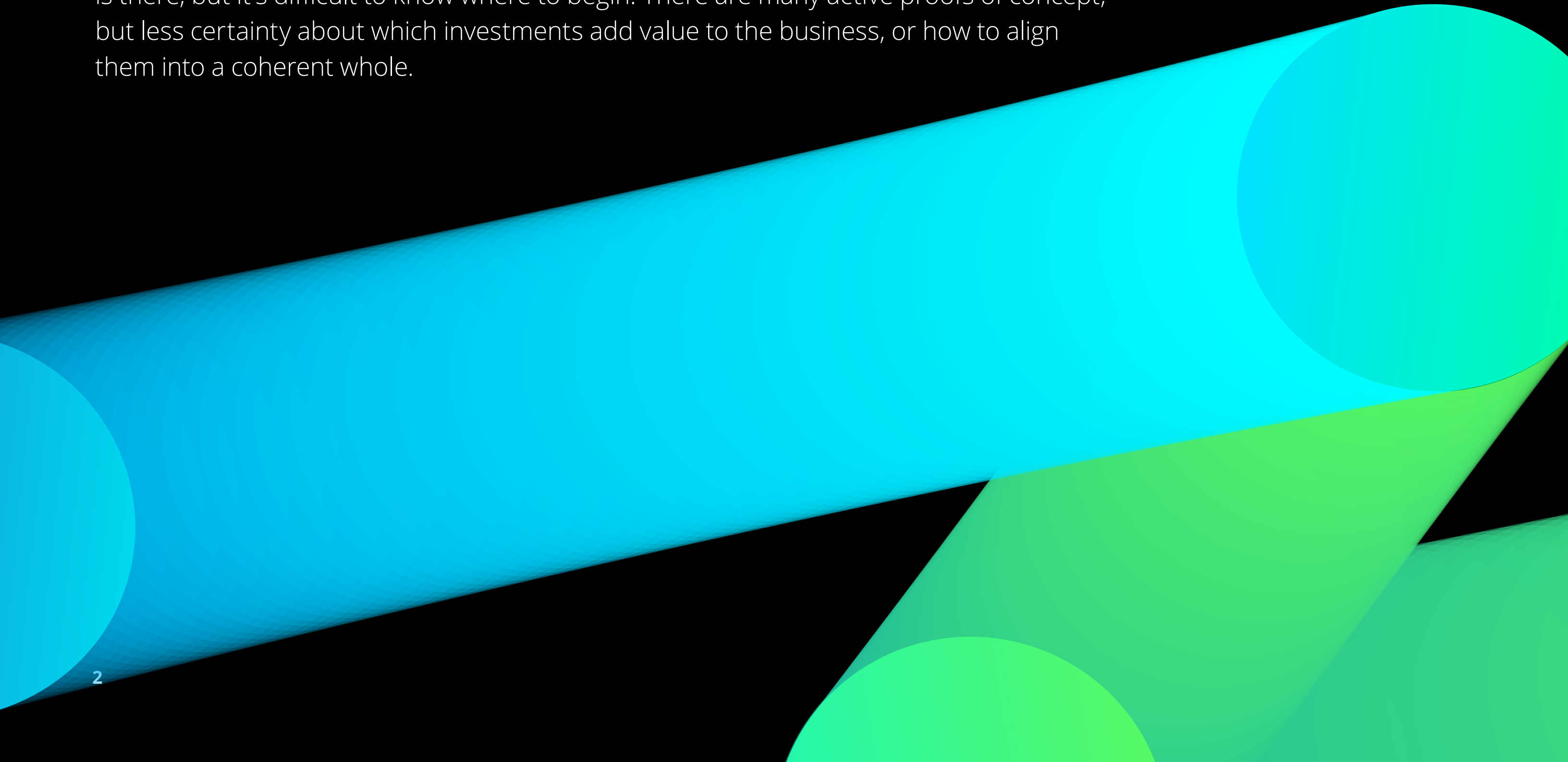
Addressing industry challenges with IT infrastructure modernization

Consumers aren't the only ones who expect more from banks. So do the banks themselves. They want to offer the agile, open banking environment that attracts business. They want to strengthen regulatory performance, bolster security, streamline development of new offerings, and keep costs under control.

Central to all these ambitions is the information technology infrastructure a bank relies on. The predominance of siloed, batch-based, monolithic architectures has left many institutions limited in their ability to adapt. Compliance and security remain preeminent concerns, and legacy architectures make it harder to be flexible and responsive in those areas. Meanwhile new market challengers are often cloud-native, which gives them the high degrees of scalability and flexibility they seek but lack.

Modernizing a bank's IT architecture by moving to the cloud can open the door to capitalizing on artificial intelligence (AI) solutions and meeting customers at their point of need, restoring balance to the playing field. Banks that have taken this journey have seen cost reductions of as much as 60% compared to their legacy systems, freeing resources they can devote to customer acquisition and digital competitiveness. Banks that have not made this leap may risk being left behind the competition, and customers may perceive them as slow, lacking in innovation, or unresponsive to their fast-changing needs.

What's stopping every bank from taking on this transformation? In some cases the will is there, but it's difficult to know where to begin. There are many active proofs of concept, but less certainty about which investments add value to the business, or how to align them into a coherent whole.



First things first: Core architecture principles for modern banking systems

While every bank will have unique needs to address in its IT architecture, there are common approaches that AWS and Deloitte have found can help in forming the foundations most institutions will build on. These include:

Defense in depth
Microservices and event-driven architecture
High availability and resiliency
Automated infrastructure and delivery
Security and compliance

Defense in depth

Traditional architectures place security barriers only at perimeter entry points, then allow users to navigate within the system after an initial credential check. This is no longer stringent enough to safeguard complex systems and data against advanced threats. The new approach imposes defense in depth through "zero trust"—meaning that even when someone is "in," the user must secure authentication and authorization at each step.

A banking platform fortified in this manner has a smaller "attack surface," enhanced compliance, and less vulnerability to fraud. This "never trust, always verify" model can not only make it more difficult for unauthorized users to exploit any initial gain of access, but also give a bank more control over the different levels and kinds of authorization its own personnel are meant to use. While "zero trust" overall is just one principle of sound banking IT architecture, it also has internal principles of its own:

No implicit trust: You're an employee? An authorized contractor? An admin? Please revalidate your credentials anyway, at every step. Zero trust means what it says: Every access request requires confirmation according to security and risk policies. No user, device, application, location, or network connection gets an exception.

Least-privilege access: Each user, device, and application receives only the minimum level of access—the "least privilege"—required to perform the intended function at the intended time.

Multifactor Authentication (MFA) and Role-Based Access Control (RBAC): combine to provide a layered approach to secure user access. MFA helps ensure that only authenticated and authorized users can access resources, while RBAC governs the specific permissions and access rights those users can have based on their roles and responsibilities.

Micro-segmentation: divides networks into small, secure zones that limit lateral movement and reduce the risk of a widespread breach.

Continuous monitoring and validation: Zero-trust architecture continuously monitors and validates user, device, and application behavior and revokes or restricts access if anomalies or threats are detected.

Context-aware access: Access decisions are based on contextual information, such as user identity, device posture, location, time of day, and the sensitivity of the requested resource.

Microservices and event-driven architecture

Traditional architectures are monolithic, with large, tightly coupled applications. That can be convenient in the moment of use, but it can make incremental updates, up- or downscaling, and resilience more difficult. These structures present a single point of failure, which can translate into their biggest inherent risk. A different approach, microservice architecture, breaks down or "decomposes" an application into its constituent parts: a collection of small, loosely coupled, and independently deployable services. Each microservice encapsulates a distinct business capability or domain function that communicates with other services through well-defined interfaces and protocols.

Breaking down an application this way can help make resource allocation more efficient and make it easier to scale based on demand. That can improve performance across various channels. Decoupled microservices promote resilience as well, since the failure of one service doesn't cascade automatically to the entire application.

Microservices architecture doesn't only protect; it can help create. Services can be reused like building blocks across different applications or contexts, reducing duplication of effort and promoting code reuse, which is beneficial in omnichannel systems where consistent experiences need to be delivered across multiple touchpoints. Creating capabilities in this way avoids the risks of larger, monolithic deployments and can bring into play patterns and practices such as service meshes, sidecar proxies, and API gateways to manage interservice communication, security, and cross-cutting concerns.

High availablity

In a nutshell, availability depends on **resiliency**—the ability to withstand or recover from failure—and **redundancy**—the ability to work around it without interruption. These are critical characteristics for an always-on banking operation that requires continuous service even when failures or interruptions occur. **One way to accomplish this in practice is to deploy redundant infrastructure** across multiple regions, or availability zones, to help mitigate the risk of downtime due to network issues, hardware failures, or natural disasters.

Load balancers are another tool to enhance resiliency and redundancy. They distribute incoming traffic evenly across multiple back-end servers while monitoring server health. If an unhealthy instance arises, the load balancer automatically redirects traffic to healthy locations and automatically scales capacity to grow or shrink based on consumption as it changes.

Capacity is another element of availability. A platform designed with scalability and elasticity, often through cloud deployment or containerization, can adjust to changes in demand. Containerization offers additional benefits such as resource efficiency, isolation, consistency, microservices architecture, scalability, and portability. Taking advantage of this elasticity doesn't happen by itself, though; **auto-scaling mechanisms** are required to provision or de-provision resources based on real-time workload monitoring.

It isn't merely computing capacity that should be reliably available. Its contents should be as well. Customer trust, regulatory compliance, and seamless operations depend on the integrity, consistency, and availability of **data**. Comprehensive data replication strategies can promote data consistency across multiple locations or data centers, and regular backups of critical data and applications—full, incremental, or differential, based on requirements—can permit rapid recovery in case of disasters.

For visibility into performance—and possible threats—comprehensive logging, metrics, and tracing mechanisms should apply across all components and layers of the platform. Advanced analytics and visualization tools can provide insights into system health, performance, availability metrics, user behavior, and transaction patterns across all components, while real-time alerting mechanisms notify administrators of issues, anomalies, or degradations that might affect performance. Machine learning and anomaly detection techniques can amplify the ability to identify potential issues or security threats.

Automated infrastructure and delivery

Automation works when it is comprehensive, from the lowest level on up. From the infrastructure that deploys into the environment to the configurations to all microservices, everything is treated as code—code that goes through rigorous peer reviews, automation testing, and security that scans it for vulnerabilities and security before it even gets sent to the environment.

Automating the Software Development Life Cycle (SDLC) process is an important step that can streamline and improve the software development processes by reducing manual errors, accelerating time to market, and enhancing overall productivity. Proper release management can prevent faulty components of a solution from being deployed to production, which can cause downtime. Global-scale events that involved flawed updates have illustrated the importance of such a safeguard.

Security and compliance

Security, compliance, and risk management call for a comprehensive approach when building a banking platform. Tools such as the AWS Well-Architected Framework can provide a consistent approach to help make infrastructures secure, high-performing, resilient, and efficient on the cloud. Whatever tools a bank uses, evaluate and monitor third-party vendors and service providers for their adherence to appropriate security and compliance standards.

Strict contractual requirements and regular audits or assessments can help make sure the platform adheres to applicable regulations and industry standards such as the Payment Card Industry Data Security Standard (PCI DSS), the General Data Protection Regulation (GDPR), and relevant banking regulations in a given jurisdiction. Other widely adopted architectural frameworks like the National Institute of Standards and Technology (NIST) Cybersecurity Framework and the Center for Internet Security (CIS) Critical Security Controls can provide valuable guidance and best practices for enhancing cybersecurity posture to build secure banking application.

Banking innovation can accelerate on the cloud

Security, availability, scalability—all of these principles can be more or less difficult to uphold depending on where and how a bank constructs its platform.

Operating on the cloud enhances a bank's ability to be efficient and agile with innovation and bringing new products and features to the market. For customers, it opens the door to the frictionless and personalized experiences they want. And for the institution, cloud architecture makes security and compliance at scale easier to achieve and maintain. In almost every case, that development is faster, and its outcomes stronger, in a cloud environment. In almost every case, that development is faster, and its outcomes stronger, in a cloud environment..

Putting the principles into practice

Recognizing the need for banks to modernize rapidly, without compromising on security, Converge™ by Deloitte BankingSuite provides banks with a secure, stable platform to lay the foundations for future growth and new capabilities.

Banks need the ability to innovate to attract increasingly demanding and well-informed customers. By solving the hard problems behind the scenes of a modern bank, BankingSuite allows clients to focus their attention and concentrate their efforts on what matters to their customers and ultimately their shareholders most. All of this happens in alignment with cloud leading practices that provide defense in depth and zero trust application architecture using AWS components to manage the security technology estate without excessive overhead.

Look again at the five principles that can guide the design of an effective architecture for banking:

Defense in depth
Microservices and event-driven architecture
High availability and resiliency
Automated infrastructure and delivery
Security and compliance

The combination of BankingSuite and AWS services with the cloud and cyber strengths of ConvergeSECURITY addresses these needs by design. Details of this combined operation includes:

- **The Amazon API Gateway** is configured with authorizers on all required endpoints to verify incoming requests for proper authentication and authorization and integrates with a Web Application Firewall (WAF) to protect APIs from common web exploits like SQL injection, cross-site scripting (XSS), and other application-level attacks.
- **Customer credentials** are managed using Amazon Cognito with a Challenge-Response Authentication Mechanism (CRAM) approach. This provides a configurable MFA platform for customers that also supports device authentication and a custom grant flow, aligned with AWS best practice guidelines, to enable biometric authentication on the WebAuthn protocol. Cognito allows organizations to associate individual users' activity logs from advanced security features with their devices, and allows users to use a previously registered device as one factor to expedite the authentication process without compromising on security and trust.
- **A zero trust approach** to the service mesh is provided by Istio, and enhanced container security is provided by a Calico firewall. The mesh employs a deny-by-default network policy. Mutual TLS (mTLS) certificates secure all traffic within the cluster, mitigating man-in-the-middle (MITM) and insider attacks. Additionally, all egress traffic from the platform is on an allowlist basis, finely controlled for specific services.
- **The Converge by Deloitte BankingSuite platform** incorporates a set of Open Policy Agent (OPA) policies to enforce best security practices within containers, automatically rejecting any image that has not been built according to established guidelines, such as using a hardened base image or being sourced from anywhere except the container registry in ECR or Kubernetes configurations that deviate from CIS or NIST leading practices and limiting deployment of unverified or untested containers.
- **The platform is controlled through fine-grained RBAC and Active Directory (AD) integration**, ensuring a consistent just-in-time least privilege process and session-based access. Secrets and keys are stored in AWS Secrets Manager and Key Management Service (KMS) with fine-grained access control and automatic rotation.

Building for the future on a flexible foundation

Customers don't see the work that goes into IT architecture, but they feel its effects. If a service or access point goes down, a bank can lose credibility and business very quickly. Customers may not know the details of a bank's security posture, resiliency stance, or disaster recovery planning, but they know whether or not they feel their money is safe. A failed login or an erroneous message may be all it takes to dispel that feeling and send them somewhere else.

Financial organizations understand this, and many know they need to modernize their platforms, but they struggle with where to start. They know they want a clearer sense of which technology improvements will drive meaningful business outcomes. And they know design decisions they make today may circumscribe or determine implementation decisions down the road they have yet to confront.

Meeting this challenge takes not only a clear view of the component technologies, but also the ways they come together. What the customer does not see, but what the bank's reliability and service ultimately rely on, are the architectural attributes that make a banking platform an accelerator and even a launchpad for service and innovation—such as microservices that can be reused in different contexts without coding them from scratch each time, which helps keep user experience consistent across touchpoints, or the composability that allows component services to be assembled in different ways as needed.

A platform with the right fabric can make sense of the whole and fill gaps among the different tools that operate on it. Increasingly, the answer to that mandate lies with agile, modular operations on the cloud in place of large, on-premise systems. When a bank turns to Converge by Deloitte BankingSuite platform solutions deployed to the AWS cloud and its cloud-native services, it can provide configurable platforms that deliver banking solutions swiftly—because the fundamental needs of building or modernizing a bank, such as scalable cloud infrastructure, security, and integration, have already been addressed.

Authors

Jack Forman
Director
Deloitte MCS Limited

Hakam Haddadin
Specialist Leader
Deloitte Consulting LLP

Adam Kolbert
Senior Director
Deloitte MCS Limited

Andy McKee
Director
Deloitte MCS Limited

Michael Michaelides
Managing Director
Deloitte Consulting LLP

James Wardle
Director
Deloitte MCS Limited

Taehyun (TH) Her
Financial Services Principal
AWS

Simon Philips
Financial Services Principal
AWS

About Amazon

Amazon is guided by four principles: customer obsession rather than competitor focus, passion for invention, commitment to operational excellence, and long-term thinking. Amazon strives to be Earth's Most Customer-Centric Company, Earth's Best Employer, and Earth's Safest Place to Work. Customer reviews, 1-Click shopping, personalized recommendations, Prime, Fulfillment by Amazon, AWS, Kindle Direct Publishing, Kindle, Career Choice, Fire tablets, Fire TV, Amazon Echo, Alexa, Just Walk Out technology, Amazon Studios, and The Climate Pledge are some of the things pioneered by Amazon. For more information, visit amazon.com/about and follow @AmazonNews.

About Deloitte

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee, and its network of member firms, each of which is a legally separate and independent entity. Please see www.deloitte.com/about for a detailed description of the legal structure of Deloitte Touche Tohmatsu Limited and its member firms. Please see www.deloitte.com/us/about for a detailed description of the legal structure of Deloitte LLP and its subsidiaries. Certain services may not be available to attest clients under the rules and regulations of public accounting.

This publication contains general information only and Deloitte is not, by means of this publication, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor. Deloitte shall not be responsible for any loss sustained by any person who relies on this publication.