BROADCOM SOFTWARE

WHITE PAPER

ENSURING REGULATORY COMPLIANCE IN HYBRID CLOUD BANKING OPERATIONS

Considerations and Strategies for Financial Services Organizations

BROADCOM SOFTWARE

TABLE OF CONTENTS

Ensuring Regulatory Compliance in Hybrid Cloud Banking Operations

Considerations and Strategies for Financial Services Organizations

Cloud computing opens new doors for accelerated transformation, innovation, and more across industries. Many financial services institutions (FSIs), in particular, leverage the cloud to roll out new products and services as they pave the way for digital banking experiences.

As the cloud increases the complexity of their IT environments, financial institutions like banks, lenders, trading companies, wealth management firms, and many other FSIs must keep up with a long list of ever-changing regulatory and compliance requirements. They also need agile, resilient infrastructures to protect critical data from internal and external threats, even as those threats evolve and span across on-premises and cloud operations.

Broadcom Software is deployed throughout financial services organizations around the world. We understand the multi-faceted complexities of simultaneously managing hybrid cloud environments and evolving regulatory compliance requirements. In this white paper, we'll explore key considerations for compliance and hybrid cloud adoption in the financial industry and share strategies for successful planning and implementation.

Considerations for Compliance in the Cloud

More than eighty percent of FSIs are already operating in hybrid cloud environments[1]. However, maintaining compliance in these spaces remains a critical and complex initiative.

The cloud helps these organizations modernize their IT environments, accelerate performance and innovation, and reduce operating costs. It also poses new challenges related to consistency, privacy, and regulatory compliance.

In fact, regulatory compliance shapes migration strategies and long-term cloud enablement roadmaps, dictating which applications move to the cloud, when migration occurs, and how to maintain each app over time.

REGULATORY COMPLIANCE SHAPES MIGRATION STRATEGIES AND LONG-TERM CLOUD ENABLEMENT ROADMAPS

To successfully embrace the cloud and maintain regulatory compliance, FSIs must consider several critical factors.

Meeting Complex, Multi-Level Regulations

The financial industry is highly regulated by varying local, regional, national, and international mandates, each of which impacts how FSIs safeguard their infrastructures from threats.

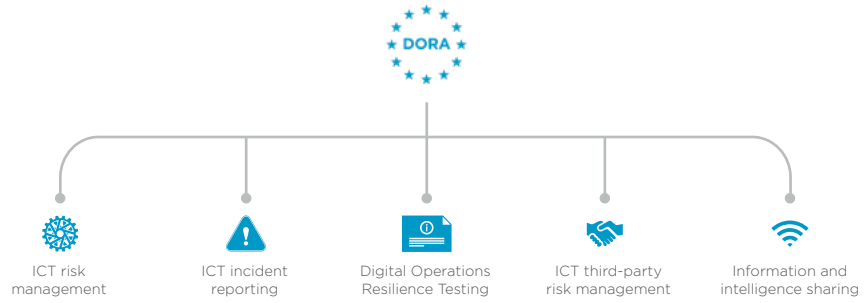
Global organizations must juggle an array of regulations with agile strategies and frameworks that meet the regulations of each geography individually without compromising the others. Not only are these regulations complex, but they also tie back to stringent audits that directly relate to an institution's reputation and ability to support its customers effectively.

Banks need to meet complex regulations like PCI DSS whether they operate globally or in a single region. Hybrid cloud architecture allows them to store data in multiple private and public clouds while centralizing monitoring, maintenance, and reporting. It also gives IT administrators complete control over which pieces of information are sent to public cloud resources.

1. Source: IDC: "Powering Financial Services Innovation With a Hybrid Multicloud Strategy."

Various regional compliance regulations, such as the Digital Operational Resilience Act (DORA) in the EU, continue to inform how financial institutions and their technology partners standardize operations, protect sensitive data, and measure performance.

The European Banking Authority Guidelines (EBAG), a predecessor to DORA, already provides regulatory guidance to FSIs in Europe. However, DORA will bring about a common approach to cybersecurity and governance for financial service providers and their IT supply chain across all the countries in the EU.



Balancing Past and Future IT Costs

As the pace of innovation increases, so do associated investments and recurring operational costs. Historical investments in on-premises software also impact how financial organizations build their technology roadmaps and IT budgets.

IT ADMINISTRATORS MUST DEVELOP HYBRID STRATEGIES THAT MAXIMIZE THEIR EXISTING SOFTWARE INVESTMENTS AND OUTLINE STRATEGIC CLOUD BUDGETS

Most FSIs already have spent a significant amount on technologies and on-premises infrastructures, which means moving to the cloud may seem costly and complicated. What's more, the mainframe offers highly secure data protection and transaction applications that don't require cloud-native architecture and will integrate with cloud-based CX apps.

Rather than abandoning the potential benefits of the cloud or their existing mainframe solutions, IT administrators must develop hybrid strategies that maximize their existing software and infrastructure investments and outline strategic cloud budgets.

Financial firms should look for ways to connect the dots between vital functionality and cloud-based applications. They should modernize and integrate essential mainframe applications into a hybrid architecture to ensure compliance, protect critical customer and business data, and drive strategic growth.

This approach not only balances out IT costs; it also yields more impactful results with fewer security risks, ensuring they maintain customer trust and minimize business disruption.

Managing Risk and Shifts in Control

FINANCIAL FIRMS MUST FIND PROVEN WAYS TO MANAGE AND REDUCE RISK IN INCREASINGLY COMPLEX ENVIRONMENTS AND DISTRIBUTED TECHNOLOGY STACKS

Financial institutions are inherently risk-averse. Their conservative approach to business operations often delays the adoption of new tools and technologies, even when the benefits of each innovation are well-documented and proven within the industry.

The cloud, in specific, requires that FSIs relinquish total control over the software and associated information in their data centers and place trust in their cloud service providers (CSPs) to deliver data protection and ensure compliance.

Since FSIs retain all the risk in a cloud environment, building trust with their CSPs is typically a time-consuming, expensive roadblock to embracing the cloud. As FSIs migrate to the cloud or expand their cloud footprint, they must find proven ways to manage and reduce risk in increasingly complex environments and distributed technology stacks.

Creating a Regulatory Compliance Roadmap in the Cloud

As FSIs strive to balance the risks of the cloud with its multi-faceted benefits, they must consider the individual applications that live in the cloud as well as the data regulation they'll use to govern them.

IT leaders at these organizations should work with other stakeholders to answer questions like:

- Which applications are best suited to move to the cloud?
- How do we leverage cloud-native technology in tandem with existing infrastructures?
- How do we federate data controls across multiple clouds?

No matter their specific IT needs or current cloud strategy, several essential guideposts can help financial firms create a compliance-focused hybrid cloud adoption plan.

Define Operational Goals and Requirements

There's no one-size-fits-all approach to hybrid cloud adoption, especially when compliance is at stake. FSIs invest in the cloud for a variety of reasons, but each firm should build its migration plan and timeline around its specific operational goals.

Most of the time, cloud migration centers around a common theme or motivation. Examples include:

Cost and Effiency

Moving to the cloud to reduce operating costs and increase operational efficiency.

IT Modernization

Consolidating infrastructure and centralizing the monitoring and maintenance of IT assets.

Accelerated Innovation

Equipping the organization with the advanced technology needed to speed up innovation and improve service delivery.

Integration Capabilities

Enabling seamless, multi-source integrations with other tools or systems that are critical for customers or employees.

Functional Requirements

Adopting the cloud to support specific technical functionalities, whether part of a strategic business plan or due to the requirements of another application in the tech stack.

IT administrators should outline their organization's goals, requirements, and constraints at the start of any cloud-focused initiative, whether they plan to migrate the entire enterprise or several core capabilities.

Identify Which Products Will Move to the Cloud

After outlining operational aims, FSIs must identify the specific applications or product lines that tie back to their goals or the key milestones in their adoption strategy.

FIRMS WILL NEED CLOUD-ENABLED INFORMATION, ENDPOINT, NETWORK, AND IDENTITY SECURITY SOFTWARE TO PROTECT CUSTOMER DATA AND THEIR OWN OPERATIONS

Data security is top-of-mind across feature sets. Firms will need cloud-enabled information, endpoint, network, and identity security software to protect customer data and their own operations.

These determinations should also account for the value and feasibility of bringing certain products to the cloud. Some applications and infrastructures will always remain on-premises, while others would benefit from the cloud's unique benefits.

Many factors will influence cloud viability, but compliance and regulatory use should be one of the most impactful determinants on which applications end up in the cloud, based on risk and control factors.

Beyond assessing the applications themselves, financial firms must understand each application's larger implications, including regulatory compliance requirements, connected services, service-level agreements, and more to determine private cloud or public cloud suitability.

Determine Migration Requirements

Next, FSIs must outline detailed migration requirements, including any technical constraints or limitations impacting how they will move each application to the cloud.

IT teams should carefully evaluate each application and document technical requirements, including whether code can simply be re-platformed, if it will need re-factoring, or if rewriting it entirely is appropriate. They should also identify which cloud-native services will support the newly migrated applications, as well as any associated tools or required security features.

Specific security requirements, including regulatory compliance with regional frameworks, data governance, and policy maintenance, should also be outlined ahead of the migration.

Plan For Ongoing Regulatory Changes

Financial organizations' hybrid cloud infrastructure must be as agile as the ever-changing regulatory requirements that govern their operations.

Achieving—and maintaining— hybrid cloud compliance requires continuous innovation, comprehensive visibility, and maintenance across the entire IT environment, which means FSIs must equip themselves with software that's designed to keep up with new requirements.

IT ADMINISTRATORS MUST APPROACH DEVELOPMENT WITH A COMPLIANCE-FIRST MINDSET

Rather than tacking compliance onto a post-development to-do list, IT administrators must approach development with a compliance-first mindset, implementing portfolio management solutions and maintenance tools that streamline configuration management and change across their entire technology stack.

Portfolio management solutions and automated remediation tools can help FSIs roll out policy changes universally across environments and execute remediation efforts quickly and accurately.

Find a Strategic Software Partner

FINANCIAL INSTITUTIONS NEED STRATEGIC PARTNERS WHO UNDERSTAND THE COMPLEXITIES OF THE CLOUD, NUANCES OF ON-PREMISES, AND FINANCE-SPECIFIC REGULATORY COMPLIANCE REQUIREMENTS

Successful cloud enablement relies on a combination of on-cloud and on-premises operations, which means financial institutions need strategic partners who understand the complexities of the cloud, nuances of on-premises, and the finance-specific regulatory compliance requirements that impact their clients' operations.

Rather than relying on a disjointed set of one-off software vendors and CSPs, financial institutions should find software partners who can effectively support every step of their journey to the hybrid cloud.

These software partners should strategically invest in the hybrid cloud and its ongoing innovations by acquiring implementation and support resources that understand regulatory requirements, constantly monitor the compliance landscape, and continually release updates and guidance to address new requirements as they arise.

Your partner should offer a depth and breadth of infrastructure solutions to support operations across the environment, including industry-specific security and privacy software, proactive monitoring tools, and solutions distinctly designed to accommodate the ever-evolving compliance landscape. Beyond their own capabilities, your software partner should have strategic relationships with global systems integrators who can deploy their solutions and whose portfolios integrate well with services.

Your Partner in Compliance Across Environments

The Broadcom Software portfolio of business-critical software is built for security and scalability. Our solutions enable customers to seamlessly combine on-premises data centers with modern, agile cloud technologies.

We provide financial institutions with advanced information, data, application, endpoint, identity, and network protection security software, including mainframe solutions, to ensure compliance plus transaction-level security and data protection for you and your banking customers.

Ready to Modernize Your IT Infrastructure for the Hybrid Cloud?

Connect with our Financial Services sales team today to discover how we can support your hybrid cloud strategy with software that modernizes, optimizes, and protects at scale.

About Us

Broadcom Software is a world leader in business-critical software that modernizes, optimizes, and protects—at scale. With its engineering-centered culture, Broadcom Software has one of the most extensive portfolios of leading infrastructure and security software, including AIOps, Cyber Security, Value Stream Management, DevOps, Mainframe, and Payment Security. Our software portfolio protects the largest financial companies in the world and enables them to deliver modern, agile, and secure services for customers and employees alike.

For more information, visit our website at: software.broadcom.com