IBM Cloud for Financial Services

Speed innovation and address your security and compliance needs

IBM

An industry facing disruption

Today, the financial services industry faces numerous disruptive forces, including ever-increasing customer demand for innovative and personalized services; intense competition from technology companies, fintechs and incumbents; rising regulatory pressure; increasing cybersecurity threats; and the need for skilled talent to address all the above.

To innovate faster and transform, many financial institutions are increasingly looking to the cloud to help them modernize existing applications, provide greater flexibility and agility, and partner with independent software vendors (ISVs), software-as-a-service (SaaS) vendors and fintechs. By fully leveraging cloud technologies, financial institutions can reshape customer experiences, streamline operations and potentially unlock new revenue models.

However, IBM has observed many financial institutions have held back from moving their core workloads and sensitive data to the cloud due to tremendous cybersecurity risk and growing regulatory complexities. According to an IBM Security-sponsored report, the average cost of a mega breach in financial services was USD 401 million as of 2021, and the average cost of a data breach rose 10% from 2020 to 2021.[1] Compromising on security or regulatory compliance is simply not acceptable.

For financial institutions to be competitive, they should continue moving core workloads to the cloud to help speed digital transformation and lower their costs, while also keeping their sensitive data and mission-critical workloads secured and compliant. To accomplish this, financial institutions need a cloud built with the specific security and regulatory compliance-monitoring capabilities the industry requires.

Financial institutions need an option that enables transparency in moving their workloads and applications to the cloud, and with IBM Cloud for Financial Services™, public cloud becomes an increasingly strategic option for efficiently speeding digital transformation.

A cloud developed for the industry

IBM Cloud for Financial Services is a first-of-its-kind public cloud developed for the industry with the security and controls capabilities to help clients as they work to mitigate risk and accelerate cloud adoption for even their most sensitive workloads.

Our cloud is designed to help clients automate their security and compliance posture and monitor it with security and controls built into the platform — not offered as add-on tools or do-it-yourself features. It also features industry-leading security and privacy capabilities and is strengthened by IBM's deep IT operations knowledge, industry expertise and an extensive set of curated ecosystem partners.

The result is a secured environment engineered to help clients with lowering the risk and cost of moving sensitive data to the cloud, modernizing workloads and rapidly integrating the capabilities needed to move their business forward.

Financial institutions can now take advantage of the benefits of public cloud while also addressing their cybersecurity and regulatory compliance requirements. There's no longer a need to choose between innovation and risk management.

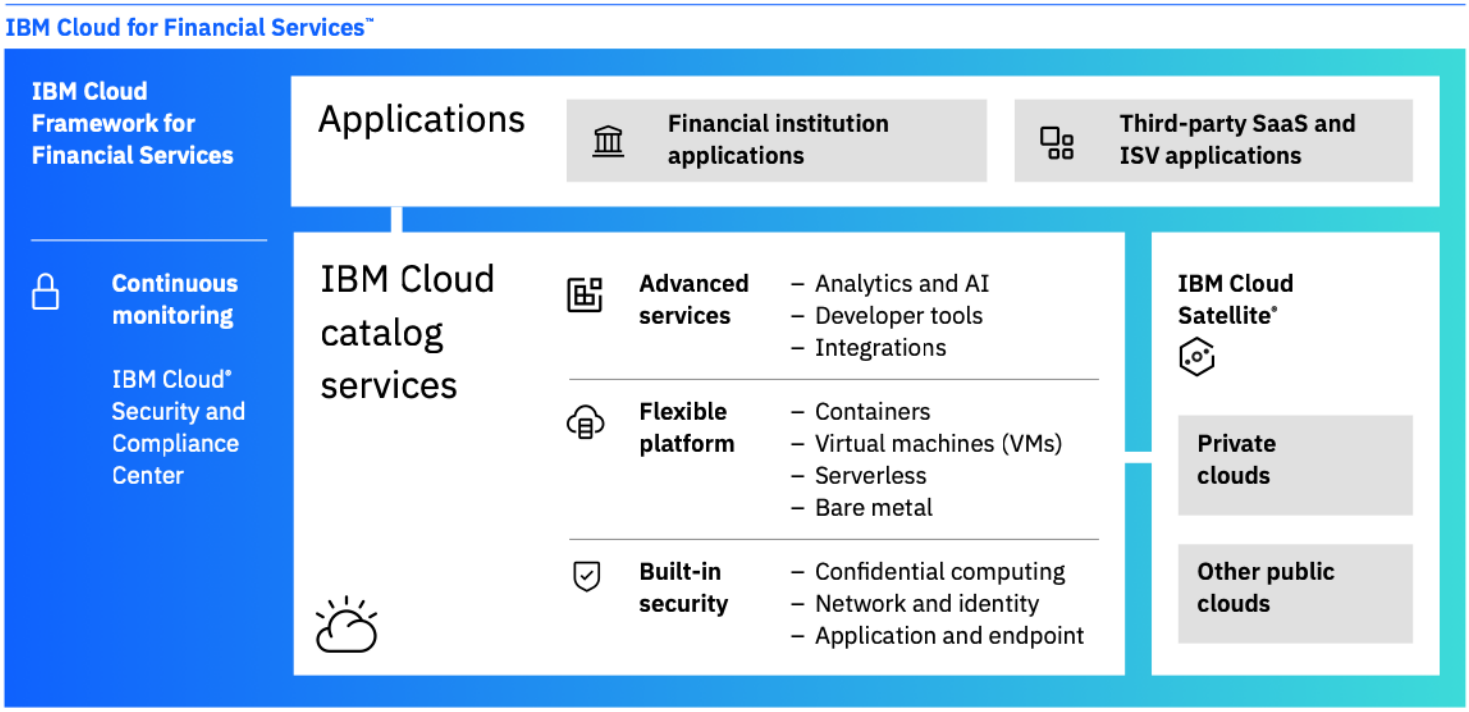
Accelerate innovation, mitigate your risk
The first cloud built in collaboration with the industry, IBM Cloud for Financial Services is designed to accelerate innovation and help lower the risk and cost of moving data to the cloud.

Address your compliance requirements with an industry-built common controls platform.

Speed innovation with an ecosystem of ISVs, fintechs and SaaS providers.

Safeguard data with industry-leading security capabilities.

Operate with choice and agility through hybrid cloud deployment options.



IBM Cloud for Financial Services leverages an industry-informed framework with preconfigured security and controls that IBM programmatically applies to the IBM Cloud services, third-party applications and institution workloads.

The controls framework, central to our platform

At the core of our offering is a controls framework called IBM Cloud Framework for Financial Services. The framework was developed to help financial institutions automate their security and compliance posture to make it easier for them and their digital supply chain partners to simplify their risk management and demonstrate their regulatory compliance.

The controls framework provides a security and compliance structure for the entire ecosystem through a common set of automated, preconfigured controls applied across IBM Cloud® services, third-party applications and financial institution workloads. Created in collaboration with major financial institutions, the controls are aligned to industry standards and global regulatory bodies. It's continually validated with advice from the IBM Financial Services Cloud Council, comprised of top financial institution CIOs, CTOs, CISOs and Compliance and Risk Officers, and guidance from Promontory Financial Group®, an IBM Company and a global leader in regulatory compliance consulting. The framework evolves, and controls are adapted to emerging industry requirements and regulatory obligations to help financial institutions as they mitigate the cost and complexity of staying compliant in an ever-evolving cybersecurity and regulatory landscape. The extensive control set within the IBM Cloud Framework for Financial Services includes but is not limited to security, data privacy, access management and configuration management.

Comprehensive controls aligned to industry standards and global regulations

7

Focus areas

- Focused risk management and compliance
- Advanced data protection
- Enhanced authentication and access management
- Automated application and workload protection
- Unified infrastructure security and resilience
- Operational excellence
- Active response monitoring

21

Unique control families

280

Controls

565

Control requirements

As of April 2022

Learn about the IBM Cloud Framework for Financial Services →

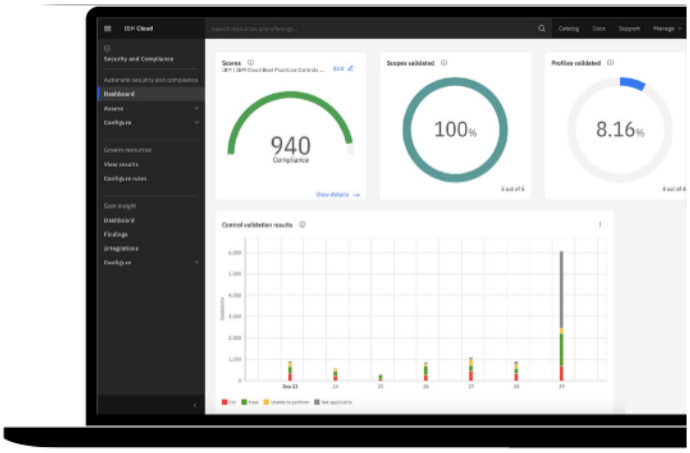
A rich catalog of ISV, fintech and SaaS solutions

IBM Cloud for Financial Services is supported by an ecosystem of curated ISVs, fintechs and SaaS providers to help make it easier and faster for financial institutions to onboard third-party applications and services and begin working with them on our cloud.

Through the IBM Cloud® Security and Compliance Center, the security and compliance postures of partner applications and services can be automated and continuously monitored and evidence captured. As a result, manual steps in the compliance-management process for partner applications can be reduced, the potential for human error minimized and consistency, traceability, auditability and scalability can all be enhanced. With automation, organizations are also able to reduce variability between audits, providing valuable, consistent reports and eliminating delays while maintaining consistent compliance.

The IBM Cloud Security and Compliance Center

The IBM Cloud Security and Compliance Center helps enable clients to monitor and enforce their controls to protect data and assets and manage vulnerabilities across cloud environments. To enable financial institutions to monitor the security and compliance posture of their cloud services, in addition to partner applications and services, IBM provides the security and compliance platform and dashboard as part of an IBM Cloud account. Clients and partners can define compliance profiles, manage controls and maintain an extensive data trail for audit. This can help promote a culture of compliance within the organization that begins with resource configuration and holds through the collection of audit evidence.



IBM Cloud Security and Compliance Center

The recent integration of Tanium Comply into the IBM Cloud Security and Compliance Center allows clients with regulated workloads to deepen their experience by having the ability to view the compliance evaluation results from Tanium from inside the IBM Cloud Security and Compliance Center. With Tanium Comply, clients can view their compliance data associated with IBM Cloud and Tanium in the same format in a single location. The Tanium integration allows IBM Cloud clients to extend their organization's endpoint management capabilities to include scanning for vulnerabilities and misconfigurations against industry security standards and vulnerability definitions.

Industry-leading security and data protection controls, with a zero trust approach

IBM Cloud for Financial Services has been designed with the exacting needs of the world's largest and most complex organizations in mind. It draws on all the data protection security capabilities and services built into the IBM public cloud, allowing it to be used for mission-critical workloads and highly sensitive data. IBM offers an enterprise-grade public cloud with extensive service-deployment options — such as VMware and Red Hat® OpenShift® as a service — and is equipped to meet the specific requirements of financial services.

Included within IBM Cloud for Financial Services are core technologies for managing security risk and regulatory compliance with a data-centric, zero trust approach.

Confidential computing
IBM takes a holistic approach to confidential computing — spanning compute, containers, databases and encryption. Confidential computing helps clients remove the implicit trust that applications place in the underlying software stack and cloud providers, so you can move from operational to technical measures and protect the privacy of your sensitive data at rest, in transit and in use. This can allow clients to move sensitive data and workloads to the cloud, unlocking new ways to collaborate and innovate. Although it's impossible to completely prevent data breaches in today's connected hybrid cloud environment, a data-centric, zero trust approach can help financial institutions modernize operations and embed security controls and is designed to mitigate the impact and cost of a data breach.

Zero trust: Built-in security across network, identity, endpoints and applications

Confidential computing from IBM: A holistic approach to protect data in transit, at rest and in use

Enabled technologies and capabilities

IBM Cloud® Hyper Protect Services IBM Cloud® Data Shield	**Keep Your Own Key** Manage keys and excrypt data with exclusive control.	**Confidential compute** Protect data in use, in servers.	**Confidential containers** Protect data in use, for containers.	**Confidential databases** Protect data at rest and in use, in data stores.

End-to-end encryption with extensive control
Our financial services cloud also offers an industry-leading key management approach that technically gives clients exclusive control of their data. Not even IBM can access it.[2] IBM Cloud® Hyper Protect Crypto Services enables cloud data encryption in a dedicated cloud hardware security module (HSM). The service offers technology like Keep Your Own Key (KYOK), a single-tenant key management service, which has key-vaulting provided by dedicated, user-controlled HSMs and that's designed to support industry encryption standards, such as Public-Key Cryptography Standards (PKCS) #11. It's also the only cloud service in the industry built on FIPS 140-2 Level 4-certified hardware. At this security level, the physical security mechanisms can provide an envelope of protection around the cryptographic module with the intent of detecting and responding to unauthorized attempts at physical access.

With this type of data protection, the client is the only party that governs and controls access to their private data. These capabilities can be game-changing for the financial services industry that needs to adhere to strict regulatory requirements for data protection.

IBM Cloud for Financial Services draws on additional services built into the IBM public cloud that also allow it to be used for mission-critical workloads and sensitive data.

Workload-centric security by default
Each workload requires various access and security rules. IBM enables organizations to define and enforce such guidelines by way of integrated container security and DevSecOps for cloud-native applications with Red Hat OpenShift as a service.

Multi-Zone Regions (MZRs)
Clients can leverage the underlying capabilities of IBM Cloud for Financial Services to enhance business resiliency and disaster

recovery. MZRs comprise multiple high-speed, low-latency, interconnected Availability Zones that are independent from each other to help limit the impact of single-failure events to a single Availability Zone, only. They enable financial institutions to locate workloads in specific geographies to fit their needs.

Logging and auditing rules
SaaS and ISV providers are required to log all actions taken through the cloud portal, API or command-line interface to be recorded in detail using IBM Cloud® Activity Tracker. This provides standard logging of activity on systems and services and full-session recording of exactly what actions operators take. This information is centrally stored and analyzed. The logging process is auditable to enable tracing of all steps, including logging both successful and unsuccessful events, and gives role-based protection at all points of intervention. The access logs are stored along with time stamps to assist analysis and forensics.

Modernizing and transforming business faster with IBM Cloud for Financial Services

To help clients modernize and transform their business faster with IBM Cloud for Financial Services, IBM meets clients "where they are" on the cloud-adoption journey by addressing the use cases most important to them, including:

- Addressing regulatory compliance across internal and digital supply chain data and workloads
- Protecting sensitive data in the cloud with a data-centric, zero trust approach
- Secured migration of virtualized workloads to the cloud
- Secured development and management of containerized, cloud-native applications

Talk to your IBM representative to take our no-cost controls assessment to understand how your financial institution's cloud or technology and security control framework aligns to IBM Cloud Framework for Financial Services. To learn more and access additional resources, visit the IBM Cloud for Financial Services web page.

Endnotes

1. *Cost of a Data Breach Report 2021*, IBM Security and Ponemon Institute, July 2021. https://www.ibm.com/downloads/cas/OJDVQGRY
2. Based on IBM Hyper Protect Crypto Services, the only cloud service in the industry built on FIPS 140- 2 Level 4-certified hardware. At this security level, the physical security mechanisms can provide an envelope of protection around the cryptographic module with the intent of detecting and responding to unauthorized attempts at physical access.

IBM Cloud
IBM Corporation
New Orchard Road
Armonk, NY 10504

Produced in the United States of America
July 2022