



The world's first
financial services-
ready public cloud

An industry facing disruption

The financial services industry is facing a number of disruptive forces—ever-increasing customer demand for new innovative products and services, competition from financial technology (fintech) companies, rising regulatory pressure and increasing cybersecurity breaches.

Venture capital flowing to fintech companies in 2018 increased 120% to USD 39.6 billion.¹ At that rate, competition in the financial services industry is expected to remain unusually intense.

Since the 2007 – 2008 financial crisis, with newly strict enforcement of regulations, the industry has incurred roughly USD 321 billion in penalties.² Governance, risk and compliance (GRC) costs account for 15% – 20% of the total operations cost of most major banks, globally.³ In short, considering the large cost of regulatory noncompliance and the need to demonstrate compliance as often as every 6 or 12 months, risk management teams in the financial services industry have a high-priority mission to evolve an IT framework that ensures successful adherence to regulations.

Similarly, while cybercrime continues to plague digital businesses across industries, financial services companies bear the highest cost, with breaches estimated to cost USD 700 billion in losses, globally.⁴ The priority is equally high for IT solutions that reduce losses related to such theft.

With those combined industry pressures, in order to create new operating and business models that can deliver innovative products and services with competitive speed, incumbent financial institutions must find ways to partner with independent service vendors (ISVs), software-as-a-service (SaaS) vendors and fintech companies themselves.



¹ [“Fintech companies raised a record \\$39.6 billion in 2018: research,”](#) Reuters, Technology News, 29 January 2019

² [“Global Risk 2017: Staying the Course in Banking,”](#) BCG, 2 March 2017

³ [“Banking Regtechs to the Rescue?”](#) Bain & Company, 18 September 2016

⁴ [“What will cybercrime cost your financial firm?”](#) Accenture, Finance and Risk, 15 July 2019

Financial services organizations require a cloud that addresses their unique needs

Like organizations in many other industries, financial institutions must improve the customer experience and modernize core applications. To transform and innovate faster, they need to be able to integrate with third-party providers.

To delight customers with personalized banking experiences and on-demand services that outpace and outsmart competitors in the delivery of services and products, organizations need the agility, resiliency, elasticity and on-demand provisioning that cloud offers.

However, as financial institutions strive to be more innovative, they also need to meet security and regulatory compliance obligations. Financial institutions, along with the ISVs and SaaS providers that service the industry, require a secure framework that instills trust and confidence in moving their workloads and applications to the public cloud.

This framework must include:

- Security and trust across the environment
- Policies and controls required to meet regulatory compliance obligations
- Complete control of data, encryption and security
- Control of intellectual property
- Control of mission-critical systems
- Portability and consistency across private and public environments
- Governance and change management driven by deep industry and regulatory expertise

Today, financial institutions are looking to the cloud to help them transform. They typically employ a hybrid multicloud cloud strategy, using both private and public clouds for their data, applications and services. With the introduction of the first financial services-ready public cloud from IBM, public cloud becomes an increasingly strategic option for safely and efficiently speeding digital transformation.



IBM has designed the first financial services-ready public cloud

In November 2019, IBM announced it had designed the first-ever financial services-ready public cloud, built on the IBM public cloud, to help address the regulatory compliance, security and resiliency requirements impacting financial institutions. It's the only public cloud

platform with a policy framework purpose-built to support financial services regulatory workloads with proactive and automated security, while leveraging the industry-leading encryption services of the IBM public cloud.

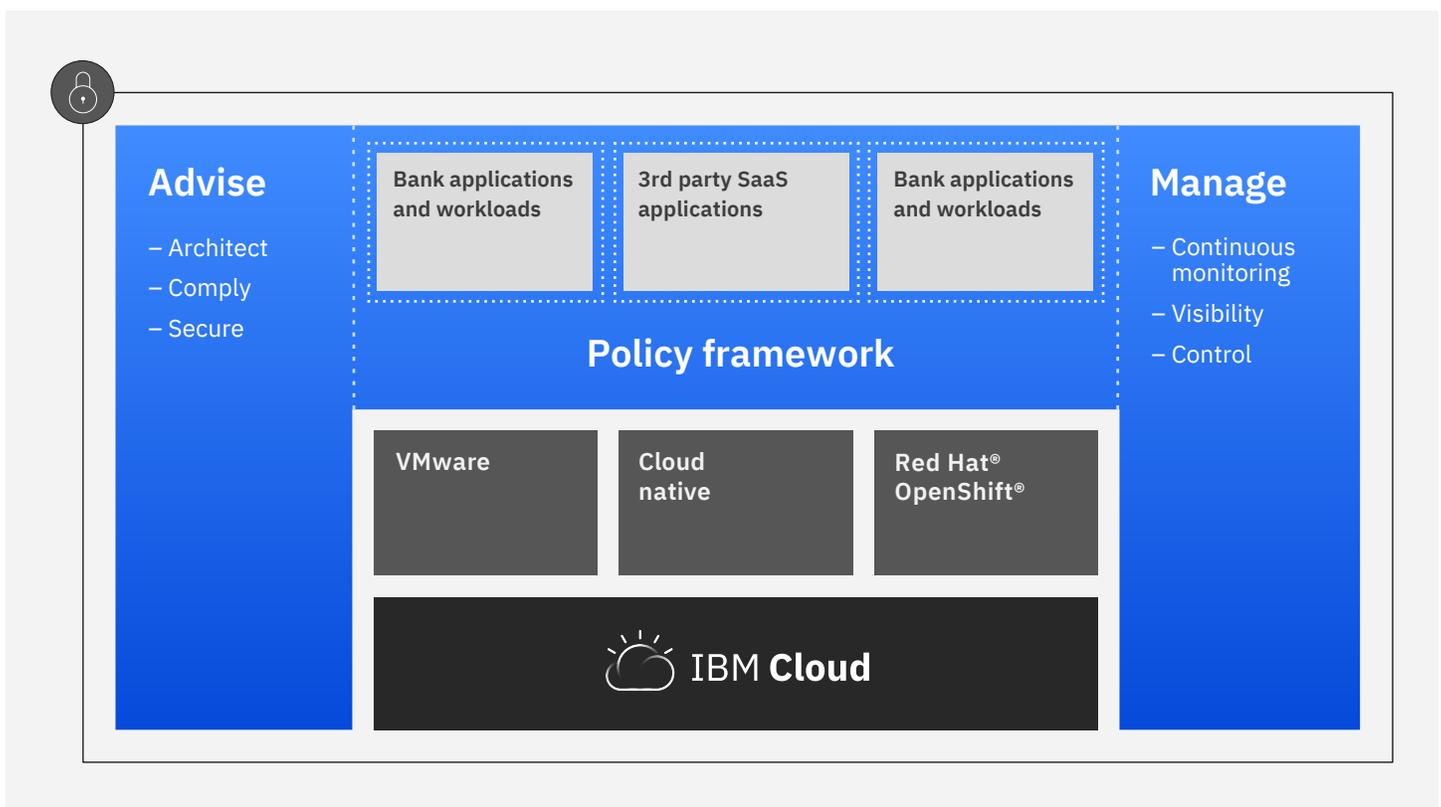


Figure 1: The world's first financial services-ready public cloud, built on the IBM public cloud

A closer look at what the financial services-ready public cloud comprises

IBM's secure and enterprise-grade public cloud

IBM's secure and enterprise-grade public cloud with extensive service-deployment options—like VMware as a service, cloud-native services and Red Hat® OpenShift®—is equipped to meet the specific requirements of financial services institutions. The capabilities of the financial services-ready public cloud are infused within the IBM public cloud. It's designed to draw upon all the data protection, security capabilities and services built into the IBM public cloud, making it ideal for mission-critical workloads and highly sensitive data.

A robust financial services policy framework

IBM's financial services-ready public cloud assists financial institutions in meeting their regulatory compliance obligations with a safe, secure, cost-effective policy framework consisting of controls to address bank security measures, regulations and rules to enforce cloud best practices.

To help financial institutions accelerate the delivery of new services to customers, the policy framework is designed with the ability to demonstrate regulatory compliance on an ongoing basis, rather than every few months.

To ensure consistent compliance across the IBM public cloud, banks and a third-party ecosystem, the policy framework deploys a shared-responsibility model for implementing controls and leverages IBM® Promontory® for ongoing governance. An IBM company and global leader in regulatory compliance, Promontory provides unparalleled regulatory expertise, counting among its ranks several senior ex-regulators.

Promontory has analyzed over 450 bank policies, industry regulations and cloud best-practice statements as input into the framework. As the IBM public cloud platform evolves, Promontory will play a key role in ensuring the platform stays ahead of changes in regulations. IBM's financial services policy framework, in combination with Promontory, reduces the cost and time financial institutions and application providers must dedicate to demonstrate initial and ongoing regulatory compliance.

A rich catalog of trusted ISV and SaaS solutions

ISVs and SaaS providers that demonstrate compliance with the policy framework will be eligible to deliver offerings through the IBM Cloud® platform. The policy framework's shared-responsibility model across all parties will enable financial institutions to move confidently to the public cloud.

The solution is designed to help reduce complexity and speed innovation for banks and providers, so that:

- ISVs and SaaS providers can spend less time demonstrating compliance and more time delivering innovative services.
- Banks can reduce overhead and the time and effort to ensure the compliance of third-party vendors, and spend more time delivering new, innovative services to their customers.
- Procurement, contracting and onboarding within the ecosystem can be streamlined, leading to increased revenues and reduced time to market for all parties.

Adopt the IBM public cloud for mission-critical workloads today

Preferred for today's hybrid multicloud environments, the IBM public cloud has the scalability, security, integration and resiliency required to run clients' most critical workloads, without compromising visibility or control, and with the data isolation they need. Whether refactoring heritage applications with Kubernetes and OpenShift or using VMware to "lift and shift" workloads from on-premises and private cloud environments to the public cloud—the fundamental platform elements remain the same.

Security leadership with market-leading data protection

The IBM public cloud has been designed with the exacting demands of the world's largest and most complex organizations in mind. It uses the same cryptographic technology that financial institutions rely on. Data that a client stores on the IBM public cloud belongs only to that client and can only be accessed by them. Clients can bring their own key that no one else can see—not even IBM—and can build and run core business applications and workloads with single-dashboard visibility and multiplatform portability, and providing:

- **End-to-end data encryption with extensive control:** IBM offers the industry's strongest commercially available state-of-the-art cryptographic technology with IBM Cloud Hyper Protect Crypto Services. The service provides the unique "keep your own key" (KYOK) capability, based on FIPS 140-2 Level 4 certification, giving clients the ability to retain control of their own encryption keys and the hardware-security modules (HSMs) that protect them.

- **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 IBM Cloud Kubernetes Service.
- **IBM Cloud Security Advisor:** This offering detects security misconfigurations so organizations can better assess their security postures and take corrective actions for all parties.

In short, the IBM public cloud is engineered with capabilities that make it the most open and secure public cloud for business.

A new standard for public cloud for financial services

With the world's first financial services-ready public cloud designed to unlock the innovation of the public cloud, while addressing the industry's unique regulatory and data protection requirements, IBM is setting a new standard of data security and privacy to help financial institutions achieve and maintain regulatory compliance. Get started today by moving mission-critical workloads to the IBM public cloud.

Receive updates about IBM's financial services-ready public cloud.

Sign up →

© Copyright IBM Corporation 2020

IBM Hybrid Cloud
IBM Corporation
New Orchard Road
Armonk, NY 10504

Produced in the United States of America
May 2020

IBM, the IBM logo, ibm.com, IBM Cloud, and Promontory are trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at “Copyright and trademark information” at www.ibm.com/legal/copytrade.shtml.

Red Hat® and OpenShift® are trademarks or registered trademarks of Red Hat, Inc. or its subsidiaries in the United States and other countries.

VMware is a registered trademark or trademark of VMware, Inc. or its subsidiaries in the United States and/or other jurisdictions.

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates.

THE INFORMATION IN THIS DOCUMENT IS PROVIDED “AS IS” WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT. IBM products are warranted according to the terms and conditions of the agreements under which they are provided.

