IBM Cloud

IBM Cloud Framework for Financial Services

1. Executive summary

As financial institutions (FIs) seek to drive improved efficiency and customer experience in an increasingly competitive and crowded market, technology transformation remains a top priority. At the same time, regulatory oversight and risk management require the risks associated with technology transformation be explicitly understood, mitigated, and managed and that the rules and regulations to which FI's are expected to adhere be continually met. These two industry drivers underpin a primary strategic imperative of FIs globally – transition to public cloud without compromising security and regulatory compliance.

With the IBM Cloud for Financial Services™, institutions can balance these priorities. IBM Cloud for Financial Services is comprised of IBM Cloud services and independent software vendor applications that comply with the IBM Cloud Framework for Financial Services (the IBM Framework).

The IBM Cloud for Financial Services helps improve efficiency and enhance competitiveness. It enables delivery against regulatory imperatives through a consistent set of embedded controls, defined as part of the Control Framework. The Control Framework is designed to meet the needs of FI control stakeholders – chief risk officers (CROs), compliance officers (CCOs), information security officers (CISOs), and data privacy officers (CPOs). It supports the strategic mandates of chief executive officers (CEOs) and chief information/technology officers (CIOs/CTOs).

2. Introduction: the context of technology transformation for financial services

FIs are subject to significant market forces tied to technology and digital innovation. Taken together, these forces have quickly become the most important drivers of change across nearly every sector of financial services. These critical factors influence the industry:

- **The rise of FinTech companies** whose ranks have grown exponentially – unencumbered by the drag effects of legacy technologies – that are able to blend 'digital first' customer demand with FI savvy.

- **Growth in innovative independent software vendors (ISVs) and Software as a Service (SaaS) providers** that harness new technological capabilities like artificial intelligence (AI) and blockchain.

- **Broader use of Cloud Services Providers (CSPs)**, using public cloud, in particular, to reduce technology debt and seize the efficiencies to enable innovation, agility, and profitability.

At the same time, regulatory pressure and risk ownership remain top priorities for regulators.

- **Regulators continue to focus on supervision and enforcement.** In the US, the Office of the Comptroller of the Currency's *Heightened Standards for Large Financial Institutions,* Federal Reserve's *Enhanced Prudential Standards*, and the Federal Financial Institutions Examinations Council (FFIEC) *Information Technology Handbook* serve as the foundation for risk management. In Europe, a number of requirements codified through MIFID II, Basel IV, LIBOR cessation, Solvency II and various European Banking Authority (EBA) guidelines achieve the same effect. Regulators in the United Kingdom and APAC continue to place similar focus on demonstrating risk management and control.

- **More data privacy statutes, rules and regulations.** These include the General Data Protection Regulation (GDPR), California Consumer Privacy Act (CCPA), Protection of Personal Information Act (POPI), Act on the Protection of Personal Information (APPI) amendments, and the forthcoming Momentum Acts— with increasingly onerous penalties, as exemplified in recent class action lawsuits regarding personal data breaches.[1]

- **Standard principles of risk management increasingly encompass the management of technology risks.** Institutions are expected to demonstrate continued adherence to requirements and expectations around resilience, third-party risk, and other factors. Here too, enforcement continues to rise, with major FIs recently subject to tens of millions of dollars in penalties.[2]

For FIs, these forces have become inextricably linked. Institutions must meet the growing demand for faster, more efficient and more streamlined technology, while demonstrating continued and strengthened risk management activities applied to IT operations, which have not always been managed in this way.

[1] Natasha Lomas, "Oracle and Salesforce hit with GDPR class action lawsuits over cookie tracking consent," Techcrunch, 14 August 2020, https://techcrunch.com/2020/08/14/oracle-and-salesforce-hit-with-gdpr-class-action-lawsuits-over-cookie-tracking-consent/

[2] Board of Governors of the Federal Reserve System "Cease and Desist Order Issued Upon Consent Pursunat to the Federal Deposit Insurance Act, as amended

3. Meeting the needs of FI stakeholders

FI stakeholders broadly agree that the public cloud represents a strategic tool to enable digital transformation, improve client experiences and enhance agility. However, these same stakeholders view the challenges of cloud migration differently.

The need to manage the priorities of each interest and the associated risks of data privacy, cybersecurity, and third-party risk, among other areas, has slowed the pace of cloud migration in financial services. As a result, FIs have moved only 16% of all workloads to the cloud, with an even smaller percentage relating to sensitive data or control processes.[3]

Overcoming these barriers requires an end-to-end capability to deliver against the needs of FIs and satisfy the interests not only of CTOs and CIOs, but also of CISOs, CROs, CCO’s and Data Privacy Officers. Each of these stakeholders have an overlapping yet distinct view of the principal risks associated with cloud.

a. CIOs/CTOs

For CIOs and CTOs, the cloud represents a launching point to enable other technologies. However, these stakeholders also manage risk and seek to protect the integrity of the FI’s IT infrastructure. In particular, migration to the cloud brings with it challenges associated with skills scarcity. Existing FI technology teams may not always possess the necessary cloud skills, thereby inhibiting an organization’s goals. These teams often must continue to support existing, on-premises infrastructure throughout the cloud migration process. And, there is a need for considerable investment to enable proper interpretation and development of controls in particular – the unique combination of skills and experience in regulation, IT risk management, and IT development is difficult to find and challenging to maintain in an increasingly competitive marketplace.

b. CISOs and data privacy officers

Similarly, CISOs and privacy officers have a key role in safeguarding sensitive data, maintaining privacy, and managing, mitigating, and preventing cybersecurity threats. With regard to migration to the cloud, the following considerations may be of primary importance:

- **Data breaches—**Unauthorized access to and disclosure of sensitive customer information may lead to significant business and regulatory impact.

- **Incorrectly configured cloud services—**Many breaches that have occurred in cloud are due to the cloud services functioning correctly, but not being configured securely, rather than a failure in cloud functionality. These configuration issues have also contributed to recent data breaches as well as ongoing fines from the U.S. Government, in one case, increasing the need for clear and easy management.

- **Incomplete data deletion—**Data spread over many different storage devices within the CSPs infrastructure in a multi-tenancy environment can complicate data deletion.

- **Internet accessible application programming interfaces (APIs) may be at risk of compromise—**The APIs that customers use to manage and interact with cloud services may be at greater risk of exploitation because they are accessible through the internet.

- **Possibility of stolen credentials—** Unauthorized access to a user’s cloud credentials can enable access to the CSP to launch further fraudulent and nefarious activity.

- **Cross-tenant exploitation—**Exploitation of system and software vulnerabilities within a CSPs infrastructure, platforms, or applications that support multi-tenancy can lead to a failure to maintain separation among tenants and jeopardize the infrastructure of the FI.

[3] CIO Surveys, Equity Analyst Research 2019-20.

c. CROs, CCOs, and other control functions

In a recent *American Banker* survey, CROs said risk management processes remain areas of global focus.[4] Migration to the cloud poses potentially elevated levels of risks that CROS and CCOs need to manage.

FIs must demonstrate continued ownership and management of risk, even when that risk is associated with third and fourth parties storing critical data or performing key processes. In a cloud-based ecosystem, CROs see this risk arising through reliance on the same CSPs and ISVs that enable the efficiencies that CIOs and CTOs seek to capture.

This risk manifests through four key characteristics of the cloud operating model:

- **Reduced Visibility and Control—**FIs lose some visibility and control over assets/ operations or both moved to the cloud, while still needing to demonstrate ownership and oversight to their regulators.

- **Adherence of third and fourth parties to FI standards—**If the CSP outsources parts of its infrastructure, operations, or maintenance, third parties responsible for these activities may not satisfy nor support the requirements of the CSP or FI.

- **IT complexity and agile development—** Operating in an agile development environment makes it difficult for risk and other second-line-of-defense functions to demonstrate their challenge and oversight as part of development efforts.

In addition to CROs, CCOs and other second-line-of-defense control functions, FIs can expect audit functions to take an interest in the processes and controls in place across all risk types as they carry out their role as third line of defense assurance functions. In some geographies, audit functions may be required to approve cloud outsourcing arrangements.

4. Introduction to the IBM Cloud for Financial Services

The IBM Cloud for Financial Services is a platform and ecosystem program designed to enable FIs and their ecosystem partners to confidently host applications and workloads in the public cloud.

To develop the IBM Cloud for Financial Services, IBM collaborated with leaders from Bank of America and Promontory (an IBM Services Company and global leader in financial services regulatory compliance consulting).

At the heart of the IBM Cloud for Financial Services is the IBM Framework that establishes a new generation of cloud for enterprises with common operational criteria and streamlined compliance controls framework specifically for the financial services industry. It’s designed to enable banks and their ISV ecosystem partners to transact with confidence.

Going beyond standard compliance and regulatory standards, the IBM Framework includes an extensive control set spanning cybersecurity, data privacy, access management, and configuration management. IBM also provides detailed guidance documentation, including reference architectures and control implementation. And policy provisions are made for continuous updates relative to changing regulatory requirements.

5. Overview of key regulatory and industry frameworks

a. Basis for the IBM Framework

The IBM Framework is based on the US National Institute of Standards and Technology (NIST) Special Publication 800-53, which provides a common control language that can be mapped to internal requirements and regulatory requirements, worldwide.[5]

These industry-informed controls will evolve to meet other internationally recognized industry frameworks, global regulatory requirements, and in particular, data privacy laws and regulations.

[4] “It’s Their Job to Worry: What Chief Risk Officers Really Think,” American Banker, https://www.americanbanker.com/slideshow/its-their-job-to-worry-what-chief-risk-officers-really-think

[5] “Security and Privacy Controls for Federal Information Systems and Organizations,” NIST, https://csrc.nist.gov/publications/detail/sp/800-53/rev-4/final

Through work with Promontory, the IBM Framework is intended to consider regulatory requirements from over 75 financial services regulators in 24 countries, including nations in North America, South America, Europe and Asia. These requirements include regulations targeted directly at cloud usage and those applicable more broadly to third-party risk management, cybersecurity and data privacy.

b. United States regulatory landscape

The IBM Framework is intended to meet the complex network of guidance documents that describe the US regulatory requirements for cloud usage by FIs. These requirements can vary depending on the nature and business of the FI. Principal among these requirements is the *Information Technology Examination Handbook (the Handbook),* issued by the FFIEC.[6] The Handbook comprises booklets on specific topics, such as Audit, Business Continuity, Development and Acquisition, Management, Operations, Outsourcing Technology Services and Information Security.[7]

The FFIEC issued its Statement on Risk Management for Cloud Computing Services, reinforcing expectations.[8] Supplementing the Handbook are related regulations and guidance issued by the Federal Deposit Insurance Corporation, Financial Industry Regulatory Authority, National Futures Association, New York State Department of Financial Services and the Securities and Exchange Commission, among others. When considered holistically, regulatory guidance in the United States outlines expectations for financial institutions to manage third-party relationships using a risk-based approach underpinned by governance, policies and procedures.

c. United Kingdom regulatory landscape

The IBMFramework is intended to meet the requirements of the Financial Conduct Authority (FCA) and Prudential Regulation Authority (PRA), the authorities primarily responsible for oversight of cloud usage for FIs. The *FCA Handbook, PRA Rulebook and Supervisory Statement SS28/15 on Strengthening Individual Accountability in Banking* outline the primary statutory requirements.[9 10 11] United Kingdom authorities have been particularly prescriptive in their expectations for cloud usage, with the FCA issuing *Guidance for firms outsourcing to the 'Cloud' and other Third-Party IT services and the National Cyber Security Centre issuing NCSC Cloud Security Principles.*[12]

d. European regulatory landscape

The European Parliament and the Council of the European Union issued a series of directives defining the statutory framework for cloud usage in the EU in addition to GDPR.[13] The European Banking Authority (EBA) and European Securities and Markets Authority have released a series of additional guidance documents, including: *EBA Guidelines on Internal Governance, Final Guidelines on the Security of Internet Payments, Final Report on EBA Guidelines on Outsourcing Arrangements, and Final Report EBA Guidelines on ICT and Security Risk Management (collectively the EBA Guidelines).*[14] Each country in the EU also issues its own implementing legislation, resulting in discrete nuances between nations.

e. Asia and Australia regulatory landscape

Regulatory oversight in Asia of cloud usage and IT-related risk occurs at the level of individual countries. Still, certain regulators have emerged as leading voices in the global cloud risk dialogue, with some proceeding more cautiously than others. For example, the Hong Kong Monetary Authority has expressed concerns regarding perceived security and consumer protection risks.[15]

[6] The FFIEC comprises the Federal Reserve Board of Governors (FRB), the Federal Deposit Insurance Corporation (FDIC), the National Credit Union Administration (NCUA), the Office of the Comptroller of the Currency (OCC), and the Consumer Financial Protection Bureau (CFPB)

[7] FFIEC IT Handbook Examination Infobase, https://ithandbook.ffiec.gov/

[8] "FFIEC Issues Statement on Risk Management for Cloud Computing Services," Federal Financial Institutions Examination Council, 30 April 2020, https://www.ffiec.gov/press/pr043020.htm

[9] "Handbook and guidance," Financial Conduct Authority, 12 August 2020, https://www.fca.org.uk/about/handbook

[10] "PRA Rulebook Online," Prudential Regulation Authority, 2020, http://www.prarulebook.co.uk/

[11] "Strengthening individual accountability in banking," Bank of England, 2015, https://www.bankofengland.co.uk/prudential-regulation/publication/2015/strengthening-individual-accountability-in-banking-ss

[12] "Outsourcing and third-party risk management," Bank of England, December 2019, https://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/consultation-paper/2019/cp3019.pdf?la=en&hash=4766BFA4EA8C278BFBE77CADB37C8F34308C97D5

[13] General Data Protection Regulation, https://gdpr-info.eu/

[14] "Final Report on EBA Guidelines on outsourcing arrangements," European Banking Authority, 25 February 2019, https://eba.europa.eu/sites/default/documents/files/documents/10180/2551996/38c80601-f5d7-4855-8ba3-702423665479/EBA%20revised%20Guidelines%20on%20outsourcing%20arrangements.pdf?retry=1

[15] https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/CloudComputing/ComplianceControlsCatalogue-Cloud_Computing-C5.pdf?__blob=publicationFile&v=3

The Monetary Authority of Singapore (MAS) has released a series of guidelines on outsourcing and IT risk management to which FI's are expected to adhere. This includes the *Guidelines on Outsourcing* issued in July 2016 and subsequently updated in 2018[16], together with *Technology Risk Guidelines* focused on cyber resilience made binding in 2019.[17]

The Australia Prudential Regulatory Authority (APRA) issued guidance in September 2018 focused on outlining specific control measures required when conducting higher risk activities on the cloud.[18]

1. Key differentiators in meeting the needs of FIs

The IBM Framework assists FIs in meeting their regulatory compliance and risk management obligations with a comprehensive framework to which ISV and SaaS providers on the IBM Cloud for Financial Services must comply. This framework simplifies and reduces the complexity of managing ISV and SaaS workloads. It specifies controls to address FI security measures, regulations and rules to enforce cloud best practices, helping FIs to demonstrate regulatory compliance faster and more efficiently. The IBM Cloud for Financial Services meets the needs of CxOs through the capabilities outlined below.

a. CIOs/CTOs

Included within the IBM Cloud for Financial Services are core technologies for managing risk, compliance and resilience risks associated with public cloud adoption, including:

- **Multi-Zone Regions—**leverages underlying capabilities of IBM Cloud for Financial Services multi-zone regions (MZRs) to enhance business resiliency and disaster recovery. MZRs comprise multiple high speed, low latency interconnected zones that are independent from each other to ensure that single failure events affect only a single zone. They enable FIs to locate workloads in specific geographies to fit their needs.

- **Isolation and segmentation—**provides compute isolation and network segmentation capabilities – meaning workloads can be deployed and managed with private-cloud-level security, within a public cloud model. Compute isolation provides dedicated servers for cloud native and VMware workloads, mitigating concerns around shared compute. With software-defined networking constructs, workloads and applications can be deployed within segmented network zones and with secure connectivity across hybrid deployments

- **Prescriptive control implementations—** Controls are prescriptive in many areas, helping teams implement applications more securely.

- **Logging and audit—**requires SaaS and ISV providers to log all actions taken through the cloud portal, API, or command line interface to be recorded in detail using IBM Cloud Activity Tracker. It 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 of successful vs. not successful 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.

[16] Electronic Banking & Technology Risk Management," Hong Kong Monetary Authority.
[17] https://www.mas.gov.sg/regulation/guidelines/guidelines-on-outsourcing#:~:text=These%20guidelines%20set%20out%20MAS,The%20guidelines%20cover%3A&text=Sound%20practices%20on%20risk%20management%20of%20outsourcing%20arrangements.
[18] https://www.mas.gov.sg/regulation/guidelines/technology-risk-management-guidelines

b. CISOs and data privacy officers

Included within the IBM Framework are the following series of controls designed to encrypt data effectively and prevent unauthorized access to cloud credentials or keys:

- **Encryption of data at rest with Keep Your Own Key—** To help prevent unauthorized access to sensitive data, IBM requires ISV and SaaS providers to agree to encrypt data at rest using the IBM Cloud for Financial Services "Keep Your Own Key" capability. Keep Your Own Key, provided by IBM Cloud Hyper Protect Crypto Services, allows customers to retain exclusive access to their encryption keys. Unauthorized parties, including IBM Cloud for Financial Services personnel, have no access to customer encryption keys at any time. In cases where a customer application encrypts data with those keys, no other parties will have access to customer data.

- **Encryption for data in motion—**To mitigate risk of stolen private keys, cloud users must agree to store the private key of the Transport Layer Security (TLS) certificates used for network encryption in the Hardware Security Module (HSM). The HSM is a tamper-proof physical device that safeguards digital keys.

  This approach aligns with Keep Your Own Key and is provided by Hyper Protect Crypto Services. Critically, private keys never leave the HSM, helping prevent unauthorized access to client keys. IBM Cloud for Financial Services is designed to encrypt connections between its services and provides encryption capability for data "in use" using Intel SGX Xeon E processors.

- **Identity and access management—**The IBM Cloud for Financial Services provides a secure and robust identity and access process for privileged administrators. It incorporates multifactor authentication and full logging of all access – which can be used for incident response and root cause analysis. By addressing the risk from privileged administrator threats, it positions FIs to support higher classification data and workloads. Customers can also use IBM Cloud Identity and Access Management to define granular access policies that reflects which identities (e.g., developers, administrators, service identities), can access specific cloud service instances and resources.

c. CROs, CCOs and other control functions

The IBM Cloud for Financial Services operates on a shared responsibility model. Typically, this model involves two or more parties, such as representatives of the IBM Cloud, one or more SaaS providers (if applicable) and the FI.
The IBM Cloud for Financial Services helps address the third- and fourth-party risk associated with this model through:

- **Standardization of controls—**The IBM Framework establishes a standard, baseline of controls set within the IBM Cloud for Financial Service, helping bring transparency to the control activities performed across the cloud ecosystem. Rather than having limited visibility into the practices of CSPs and ISVs, FIs understand that all parties are required to meet the same baseline standards set forth by the IBM Framework.

- **Clear definition of roles and responsibilities—**Within the IBM Framework, roles and responsibilities for control execution are clearly defined for the IBM Cloud for Financial Services, SaaS providers and the FI. These definitions enable clear responsibility around the controls for portion of the overall system "stack" owned by each stakeholder, as shown below.

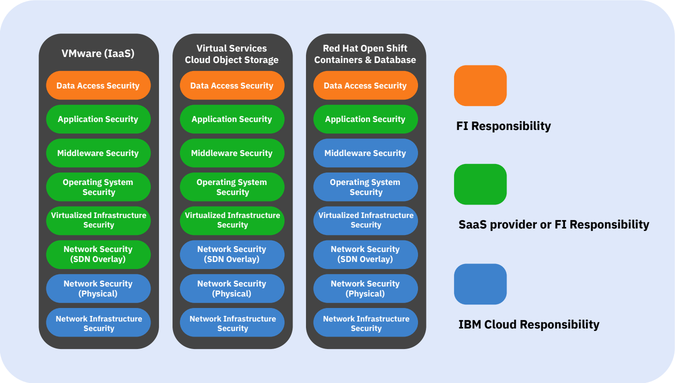

VMware (IaaS)
Virtual Services Cloud Object Storage
Red Hat Open Shift Containers & Database
Data Access Security
Application Security
Middleware Security
Operating System Security
Virtualized Infrastructure Security
Network Security (SDN Overlay)
Network Security (Physical)
Network Infrastructure Security
FI Responsibility
SaaS provider or FI Responsibility
IBM Cloud Responsibility

Figure 1. The IBM Cloud shared responsibility model indicates responsibilities for FIs in orange, SaaS providers (or FIs if no SaaS providers) in green and IBM Cloud in blue.

The definition of roles and responsibilities at the control level is more granular than that of other CSPs. The IBM Framework contains specifics on the responsibilities for each party, regarding each control with granularity that provides standardization and transparency and clarifies expectations across parties. Overall, this reduces complexity regarding third- and fourth-party risk stemming from ISVs and SaaS providers.

The responsibilities vary based on the workload pattern that is deployed, and the related technology stack that underpins those cloud adoption patterns in the financial services industry.

- **Oversight of ISVs and SaaS providers—** IBM requires that SaaS and ISV providers operating on the IBM Cloud for Financial Services demonstrate compliance against the requirements of the IBM Framework as applied to their own services. These providers also must show evidence of compliance for validation by IBM.

d. Governance and Oversight Capabilities

Regardless of risk stripe or remit, the IBM Cloud for Financial Services delivers the following comprehensive set of capabilities.

- **IBM Cloud Security and Compliance Center—**To aid in preventing compliance drift from the IBM Framework, IBM provides leading-edge tools, such as the IBM Cloud Security and Compliance Center. The tools help client cloud administrators and application developers mitigate risk and manage compliance in their use of cloud services. These administrators and developers can automate manual processes with these tools.

  Enterprise security and compliance policies can be expressed in terms of NIST 800-53 controls and a demonstrable set of implementation goals. These elements can be composed into a set of profiles applicable to FI workloads and applications.

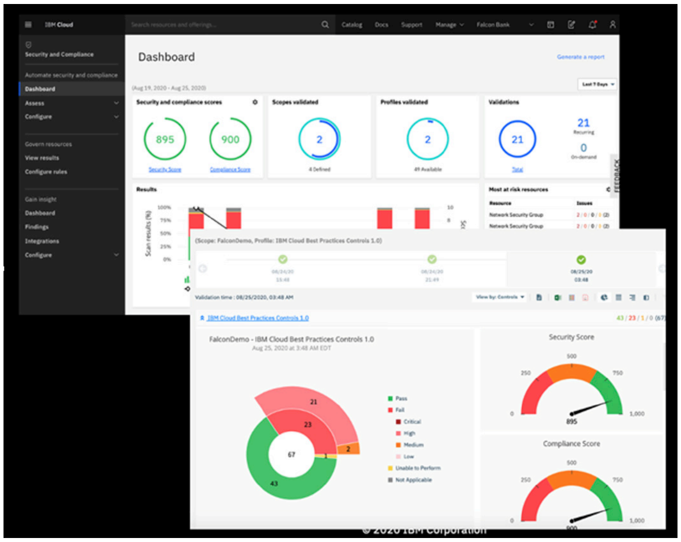


Figure 2. The IBM Cloud Security and Compliance Center shows the compliance posture of FIs.

- **IBM Framework for financial services audit—** Security executives (CISOs, CTOs and CROs) and managers of FIs using the IBM Cloud for Financial Services can gain efficiency in their internal and regulatory audits with the IBM Framework for Financial Services audit report. A third-party assessor performs periodic, rigorous assessments of the IBM Cloud for Financial Services against the IBM Framework. These assessments are more extensive than typical system and organization controls (SOC) 2 audits or SOC 3 executive summaries of SOC 2 reports. They benefit clients by offering more visibility and transparency into the control effectiveness.

2. Ongoing changes to the IBM Framework

The IBM Framework is intended to meet compliance and security requirements of supervisors globally and align with the risk and control needs of FIs. IBM Cloud for Financial Services uses two approaches to continually meet the needs of the industry:

- **Technology Compliance Advisor (TCA)—**a joint IBM Security Services and Promontory solution aimed at identifying and incorporating enhanced controls within the IBM Framework to align with changing regulatory requirements.

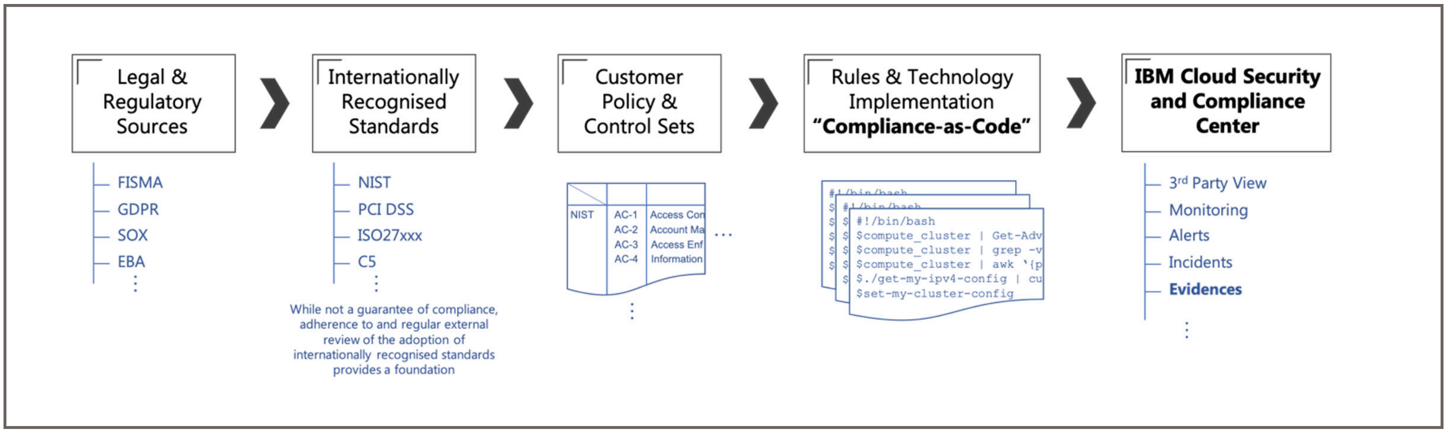
- **The IBM Financial Services Cloud Council—** The council comprises a group of senior executives from financial institutions and regulators who are leading a focused effort to advise on the ongoing advancement of the Policy Framework by contributing to and prioritizing industry requirements.

a. Managing regulatory change

IBM will actively monitor for new and changed rules and regulations, enabling the Policy Framework to remain current with the requirements and expectations of global regulators. This solution, called TCA and delivered by Promontory and IBM Security Services, includes review of the source law, identification of specific regulatory requirements, alignment to the Policy Framework and implementation of new and enhanced controls.

Where practicable, enhanced controls lead to "Compliance-as-Code" specifications, or instances where enhanced controls are automated within the IBM Cloud for Financial Services. This is enforceable in both on-premise and multiple public cloud platforms.

This process is described further in the following figure.


Legal & Regulatory Sources
FISMA
GDPR
SOX
EBA
Internationally Recognised Standards
NIST
PCI DSS
ISO27xxx
C5
While not a guarantee of compliance, adherence to and regular external review of the adoption of internationally recognised standards provides a foundation
Customer Policy & Control Sets
NIST
AC-1
AC-2
AC-3
AC-4
Access Con
Account Ma
Access Enf
Information
Rules & Technology Implementation
"Compliance-as-Code"
IBM Cloud Security and Compliance Center
3rd Party View
Monitoring
Alerts
Incidents
Evidences

```
#!/bin/bash
$compute_cluster | Get-Adv
$compute_cluster | grep -v
$compute_cluster | awk '{p
$./get-my-ipv4-config | cu
$set-my-cluster-config
```

Figure 3. How IBM Cloud applies mapping regulatory requirements and industry standards to the IBM Framework.

b. The IBM Financial Services Cloud Council

IBM announced formation of the IBM Financial Services Cloud Council to bring major financial institutions together to help drive strategic evolution of cloud security in the industry. The Council will include C-level members from large, global FIs recognized for their knowledge and awareness of best practices for security and compliance.

3. Conclusion

IBM Cloud for Financial Services is designed to build trust and enable a transparent public cloud ecosystem with features for security, compliance and resiliency that FIs require. FIs can confidently host their mission-critical applications in the cloud and transact quickly and efficiently. With an ecosystem of multiple FIs and more than 30 ISV partners to start, the IBM Financial Services Cloud Council offers a new generation of cloud for the enterprise. FIs can now deploy on public cloud to enable innovation and deliver new, more personalized customer experiences, while managing stringent industry regulations for sensitive data and complex workloads.

Core to this mission is the IBM Framework, which provides a standardized control set with clear ownership for control execution between FI clients, ISVs and SaaS providers and the cloud itself, mitigating third and fourth-party risk.

IBM Cloud
IBM Corporation
New Orchard Road
Armonk, NY 10504

Produced in the United States of America
September 2020

Contributions by IBM and Promontory,
a wholly owned subsidiary of IBM

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 MERCHANT-ABILITY, 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.