# Build a Hybrid Cloud Platform for Mainframe centric Regulated Workloads with IBM Cloud for Financial Services

*Yichong Yu, STSM, IBM Cloud for Financial Services™*
*Pradeep Kadiyala, Senior Solutions Architect for IBM Cloud for Financial Services*
*Surya V Duggirala, IBM Distinguished Engineer and CTO, Enterprise Cloud Architecture*

Most of the regulated industries use mainframes to support their core business transactions due to their time-tested qualities of service (QoS) like security, resiliency, and high availability. As evolving new business models require modernization of these core mainframe workloads, enterprises are looking for a hybrid cloud platform with strong security and compliance feature support to achieve this.

IBM Cloud is designed for regulatory workloads and works with an ecosystem of regulated clients and ISVs to continuously improve the compliance posture. IBM Cloud has many features to support Hybrid Cloud deployments and is uniquely positioned to support enterprise workloads including regulated workloads with its support for heterogeneous compute architectures like x86, IBM Z® and Power®. IBM Cloud® also benefits immensely from IBM Z platform centric enterprise cloud services offered in its catalog.

## Security and Compliance Requirements for Regulated Workloads

Financial institutions need to comply with cyber security standards, laws, and regulations to maintain a strong security posture and to prevent data breaches. There are variety of security regulations and international, federal, and regional laws. Here are some major global regulatory bodies.

| Regulatory Authorities | North America | United Kingdom | Europe | Asia-Pacific | Australia |
|---|---|---|---|---|---|
| | FFIEC, FDIC, OSFI BSIF, CSA/ACVM (Canadian Securities Administrators / Autorités canadiennes en valeurs mobilières) | Bank of England Prudential Regulation Authority, FCA Financial Conduct Authority, National Cyber Security Centre (a part of GCHQ) | EBA European Banking Authority, GDPR, enisa, BaFin German Federal Financial Supervisory Authority | Financial Services Agency, METI Ministry of Economy, Trade and Industry, FISC 金融情報システムセンター The Center for Financial Industry Information Systems | APRA Australian Prudential Regulatory Authority |
| Industry Standards | NIST | CSA cloud security alliance® | | | |
| Global Standards | PCI DSS COMPLIANT | ISO/IEC 27001 | AICPA SOC | SOC 1, SOC 2, SOC 3 | |

Financial institutions typically must comply with more than one set of requirements, and it is easy to get lost while implementing relevant IT standards, regulations, and local laws. Financial institutions also need to constantly adjust their security controls and processes to frequent cybersecurity landscape changes. It is time consuming and challenging to meet the compliance requirements and keep up with the changes.

There are many different factors to consider when designing a secure architecture in cloud, including network security, identity and access management, application security, and data security (refer to the security blog for more details). It requires deep knowledge in each area to design the infrastructure and to make sure that there are no security holes in the design.

Financial institutions need to continuously monitor the environment to make sure that they maintain a strong security posture. If there are any issues, they need to discover and fix them quickly. They

need some tools to help them with the continuous monitoring for security evaluation and evidence collection for auditing purpose.

To design and implement these security and compliance features from ground up in a cloud platform requires significant effort and resources. If there is a cloud platform that can take care of these aspects, clients can just focus on building differentiated value to their enterprise workloads and business processes.

## IBM Cloud for Financial Services

This is where IBM Cloud for Financial Services can help. IBM Cloud for Financial Services is designed to help clients mitigate risk and accelerate cloud adoption for sensitive regulatory workloads. 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.

IBM Cloud Framework for Financial Services is designed to build trust and enable a transparent public cloud ecosystem of ISVs and IBM Cloud services with the features for security, compliance, and resiliency using Security and Compliance Center (SCC) that financial institutions require. The Security and Compliance center has a set of profiles with pre-defined controls and polices that will run, monitor, and audit the services. The policies and controls are determined by IBM Cloud Regulatory Council members who are from Risk and Compliance of leading Financial Industry companies. The ISVs and IBM Cloud services are being validated by the controls defined by the regulatory council members. Once validated they become Financial Services validated. A set of reference architecture patterns are defined through Infrastructure as code (IaC) on IBM Cloud using services that are Financial Services validated.

The IBM Cloud Framework for Financial Services consists of:

- A comprehensive set of controls designed to help address the security requirements and regulatory compliance obligations of financial institutions and cloud best practices. The technology-agnostic control requirements defined in the framework were built by the industry for the industry. The framework contains 565 controls that span 7 focus areas and 21 control families. The controls were initially based on NIST 800-53 Rev 4 and have been enhanced based on feedback from leading industry partners.
- Detailed control-by-control guidance for implementation and supporting evidence to help address the security and regulatory requirements of the financial industry. IBM Cloud services or ecosystem partner services can evidence compliance to the controls and become IBM Cloud for Financial Services Validated. The Financial Services Validated designation signifies that you have successfully evidenced compliance to the control requirements of the IBM Cloud Framework for Financial Services and may improve your ability to market to financial institutions. IBM Cloud for Financial Services provides the Control Implementation Overview templates which are the definitive guides to the controls and required evidence for service providers. IBM Cloud provides a growing list of cloud services that are IBM Cloud for Financial Services Validated.
- Reference architectures designed to facilitate compliance with the control requirements. In addition, resources are provided to deploy infrastructure as code in order to automate deployment and configuration of the reference architectures.

- Tools and IBM services, such as IBM Cloud Security and Compliance Center, to enable parties to efficiently and effectively monitor compliance, remediate issues, and generate evidence of compliance.
- Ongoing governance of the framework documentation that considers new and changing regulations, as well as bank and public cloud requirements.

### IBM Cloud Security and Compliance Center

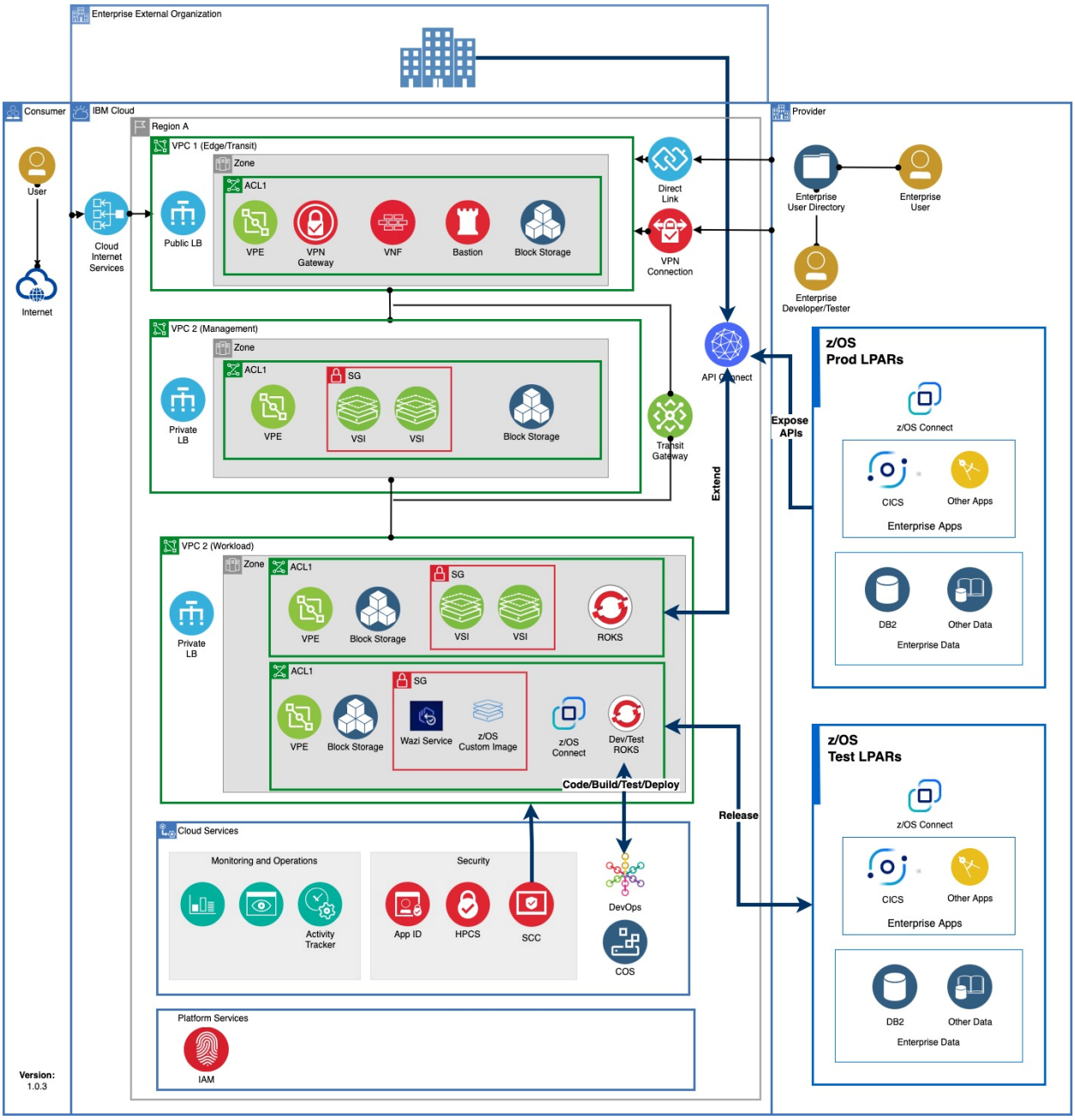
IBM Cloud Security and Compliance Center provides visibility into your workloads with features such as security and compliance automation, monitoring and assessing compliance across hybrid cloud environments, gathering evidence for compliance needs, increased visibility for your entire organization, and regular reviews for compliance audits.

Through automation, continuous monitoring and customizable profiles, IBM Cloud Security and Compliance Center is one of the unique services in the industry that provides monitoring of not only IBM Cloud Infrastructure and applications, but it also integrates with on-premises infrastructure and services. Integrating IBM Cloud centric controls with on-premises centric IBM zSystems™ controls will provide insights into a true hybrid cloud security and compliance posture.

IBM Cloud Framework for Financial Services provides three reference architectures as a basis for meeting the security and regulatory requirements. These three reference architectures include IBM Cloud Virtual Private Cloud (VPC), IBM Cloud Satellite, and IBM Cloud for VMware Regulated Workloads.

IBM Cloud Virtual Private Cloud reference architecture allows enterprises to establish their own private cloud-like computing environment on shared public cloud infrastructure. It gives two options for compute that can be mixed and matched: IBM Cloud Virtual Servers for Virtual Private Cloud and Red Hat® OpenShift® on IBM Cloud.

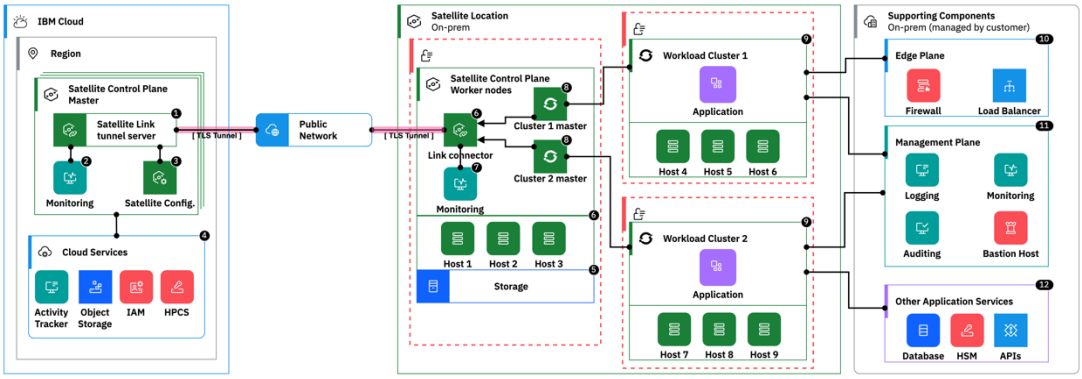
Central to the architecture are two VPCs, which provide for separation of concerns between provider management functionality and consumer workloads. On-premises centric mainframe workloads can be integrated with workloads hosted on secure regulated IBM Cloud environment using VPC architectures through various modernization patterns including API, DevOps, Data and AI. The diagram below describes high level reference architecture of mainframe application modernization using VPC Infrastructure Pattern of IBM Cloud for Financial Services.




Applications running on IBM zSystems can expose the APIs using z/OS® Connect. All the development and testing can be performed on Wazi as a service in a secure isolated environment workload VPC and deployed to Pre-Production and Production environment using IBM DevOps Toolchain. Data can be migrated using DirectLink, Event Streams and Cloud Native services available on IBM Cloud. The architecture framework provides segmentation by setting network access controls and security groups on workloads. The APIs can be extended using API Connect and security firewalls using Edge/Transit VPC. All the monitoring and auditing of the workflow flow logs can be managed from Management VPC or existing IBM Cloud Monitoring services. The IBM Security and Compliance Center (SCC) runs the compliance posture and provides alerts and auditing.

This architecture fulfills both data centric and application centric architecture patterns (reference links) in a secure regulated FS Cloud environment.

The Satellite reference architecture for IBM Cloud for Financial Services is designed to provide a framework for building Satellite-based solutions by using a shared responsibility model to fulfill the best practices and requirements of the IBM Cloud Framework for Financial Services. A key aspect of the IBM Cloud Framework for Financial Services is to separate user workloads from system management functions and isolate security functions from non-security functions. The network infrastructure of the Satellite location can be used to provide physical and logical separation between the Satellite management control plane and your workloads. You can create a hybrid environment that brings the scalability and on-demand flexibility of public cloud services to the applications and data that run in your secure private cloud.




Satellite with on-premises data center infrastructure, and IBM zSystems provide security, control, visibility, and shared responsibility, reducing the overall management and operational costs. Let's look at each of these aspects that relates to IBM zSystems.

Security:

Security on IBM Cloud satellite starts with having a secure Direct Link or TLS connection between IBM Cloud and on-prem. IBM Cloud managed services like ROKS enable you to bring modernized cloud native applications close to your core mainframe applications reducing the network latency and increasing the performance and resiliency. Network isolation between the workloads and management keeps the sensitive applications secure. Services like HPCS will allow you to Keep Your Own Key (KYOK) and use it for data encryption at-rest, in-transit, and in-use.

Control:

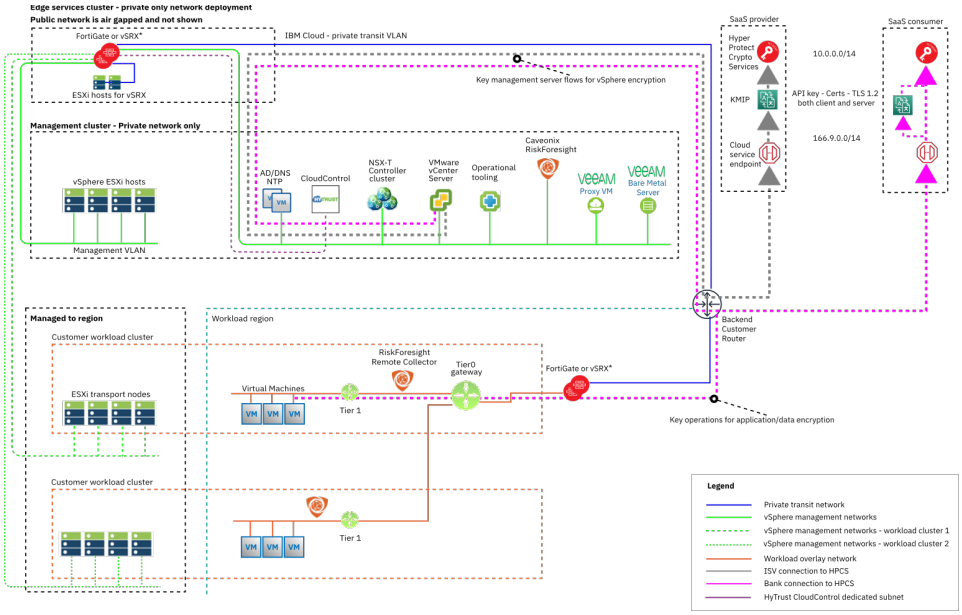
Satellite provides a shared responsibility to have complete control on your workloads and at the same time offload the operations like monitoring and maintenance capabilities to IBM Managed services.

Visibility:

IBM Managed services provide complete visibility without needing to have access to the sensitive information. The health and usage metrics of the workloads are provided, thus protecting from any outage, and enabling high resilience on the on-prem based IBM zSystems.

Shared Responsibility:
The responsibilities for deploying, operating, and securing products are shared between IBM and clients. This gives customers to have control but also reduce the operations on IBM Managed services. A complete set of shared responsibilities are being defined here.

IBM Cloud for VMware Regulated Workloads reference architecture is an extension of the VMware vCenter Server® offering. Its design extends and enhances the basic vCenter Server architecture to deliver a secure, high-performance platform. You're able to run both classic virtualized workloads and containerized applications with the addition of Red Hat OpenShift on IBM Cloud.




IBM Cloud for Financial Services includes best practices that summarize some of the most important technical principles for Software as a Service (SaaS) and software providers based on the control requirements and implementation guidance that financial institutes should follow.

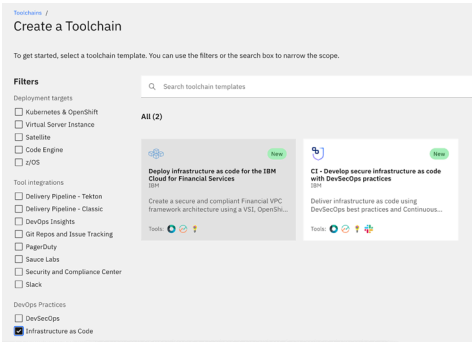
## IBM Cloud Hyper Protect Crypto Services (HPCS)

IBM Cloud for Financial Services is built on top of a network and security hardened IBM Cloud platform, leveraging IBM Cloud Hyper Protect Crypto Services. More details about HPCS can be found in the security pattern blog here.

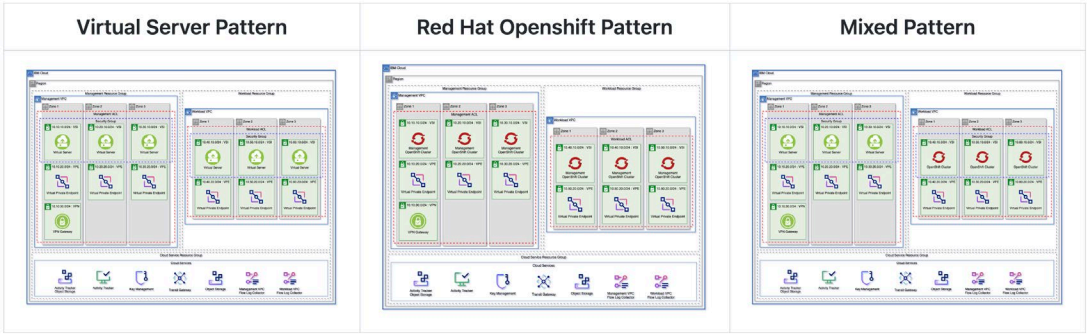
## Deploy infrastructure as code for IBM Cloud for Financial Services

It could be time consuming and error prone to deploy secure client applications in cloud from scratch. IBM Cloud for Financial Services provides DevOps toolchain to deploy the reference architecture of client's choice in IBM Cloud as Secure Landing Zone (SLZ), which meets the security and compliance requirements of financial industry and follow the best practices. Clients can then add their applications on top.

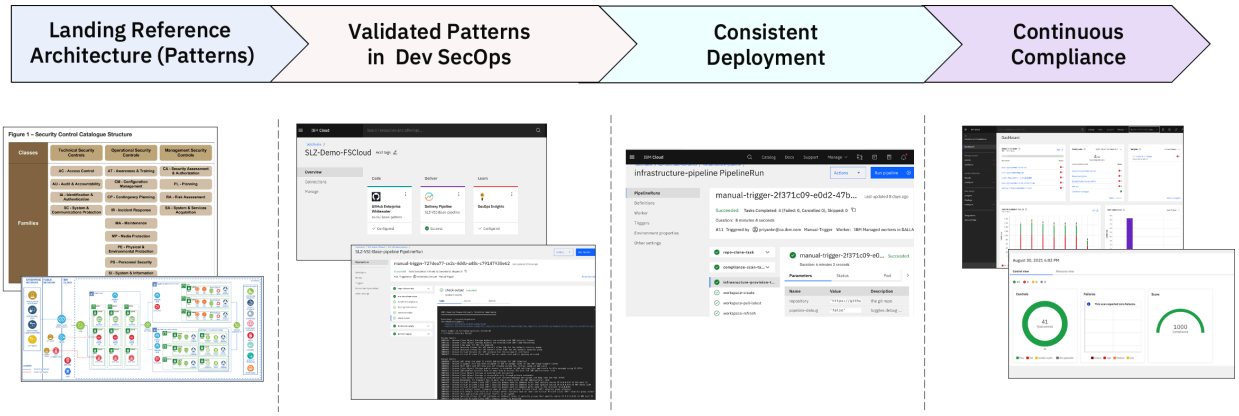
After you log in to IBM Cloud and create a DevOps Toolchain, you can find a tile to deploy infrastructure as code for the IBM Cloud for Financial Services.




The landing zone module can be used to create a fully customizable VPC environment. The three patterns below are each starting templates that can be used to quickly get started with Landing Zone. Secure Landing Zone provides sample applications that can be used to deploy into your infrastructure. These can be tied into your infrastructure provision pipeline via the application deploy task within.



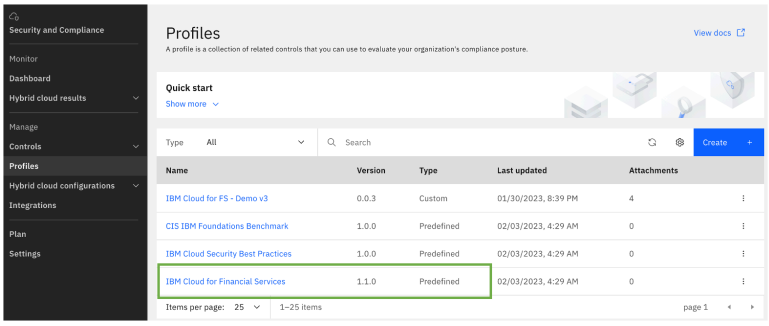

The landing zone module uses validated patterns in DevSecOps, creates consistent deployment to set up the reference architecture of client's choice. The resulting environment can be continuously monitored via IBM Cloud Security and Compliance Center.



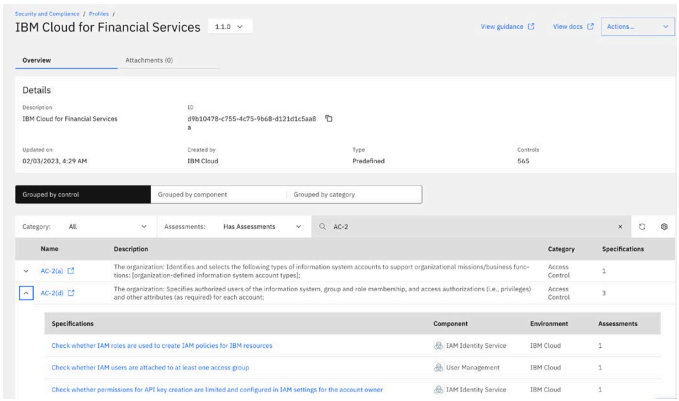
## Continuous compliance with IBM Cloud Security and Compliance Center

Highly regulated industries, such as financial services, require organizations to achieve continuous compliance and protect customer and application data. Historically, that process was difficult and manual in nature, which placed organizations at risk. With IBM Cloud Security and Compliance Center (SCC), one can integrate automatic compliance checks to help minimize the risk.

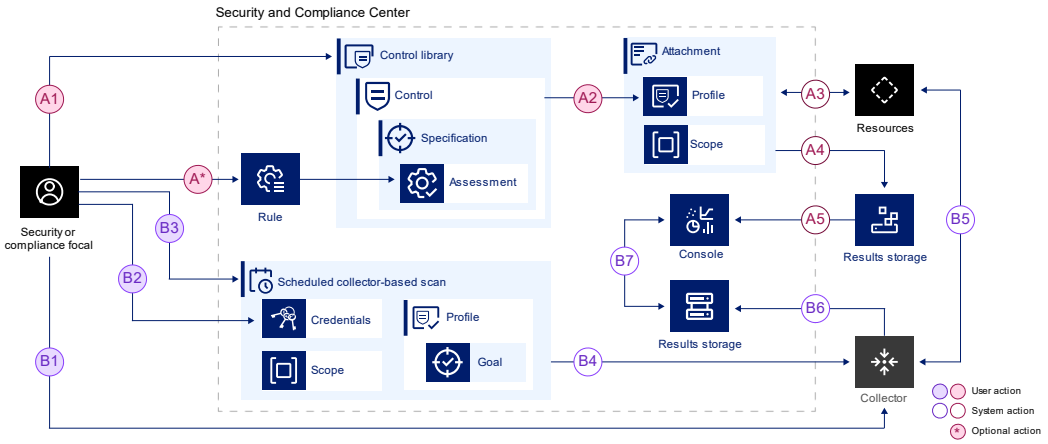
IBM Cloud Security and Compliance Center provides predefined
IBM Cloud for Financial Services profile.




The framework contains 565 control requirements that span 7 focus areas and 21 control families. The control requirements were initially based on NIST 800-53 Rev 4 and have been enhanced based on feedback from leading industry partners.




SCC is designed to help you achieve continuous evaluation of your resource configurations for potential risks. You can use the predefined profiles or create custom rules and profiles to suit your needs (A1 in the chart below). You can then create an attachment of the profile to the scope of resources you want to scan (A2). The resources will be scanned (A3) and results saved to Cloud Object Storage (A4). The results of the scanning are displayed in SCC dashboard (A5). You can check your security and compliance posture anytime and remedy risks in your environment.




## Conclusion

It is critical to protect sensitive data and workloads in cloud, yet it is challenging to design architecture and meet all the security and compliance requirements of highly regulated industries, such as financial services.

IBM Cloud for Financial Services is designed to build trust and enable a transparent public cloud ecosystem with security, compliance, and resiliency features that financial institutions require. The Financial Services Cloud framework defines a comprehensive set of control requirements and provides automation and configuration of proven reference architectures. It not only addresses the needs of financial services institutions with regulatory compliance, security, and resiliency during the initial deployment phase but also efficiently and effectively monitors compliance, remediates issues, and generates evidence of compliance for ongoing operations. The framework is also informed by an industry council and Promontory Financial Group, an IBM subsidiary, to ensure that it is current with new and updated regulations.


IBM Corporation
New Orchard Road
Armonk, NY 10504
U.S.A.
12/23