

Tags

Cloud

Making IBM Cloud fo Work for You



See how the unique industry-specific capabilities of IBM Cloud for Financial Services are designed



Hello! How can I help you?

See how the unique industry-specific capabilities of IBM Cloud for Financial Services are designed to help you reduce risk and accelerate cloud adoption.

Are you responsible for developing, deploying or managing applications and data in the financial services industry? Do you spend a lot of time worrying about all the associated risks, compliance standards and regulatory requirements? Would you rather spend more time focused on how to deliver value to your clients? If so, keep reading to learn how [IBM Cloud for Financial Services®](#) can help you mitigate risk and accelerate your adoption of the cloud.

[IBM Cloud®](#) is well-suited for regulated workloads with its [end-to-end cloud security capabilities](#) and support for a wide-range of [compliance programs](#). IBM Cloud for Financial Services extends the capabilities of IBM Cloud to provide an industry-driven cloud platform that supports the unique requirements of the financial services industry. It hosts a rich ecosystem of IBM Cloud and partner services that makes it easier to achieve and demonstrate regulatory compliance postures for your financial services workloads.

In addition, the [IBM Cloud Framework for Financial Services](#) provides the following accelerators to help you effectively use IBM Cloud for Financial Services to host even your most sensitive and mission-critical workloads:

- A comprehensive, first-of-its-kind set of control requirements designed to help address the security and regulatory compliance obligations of financial institutions.
- Detailed implementation guidance for each control requirement to go hand-in-hand with detailed reference architectures.
- Automation to make it easier to deploy and configure the reference architectures.
- Tools that enable you to efficiently and effectively monitor compliance, remediate issues and generate evidence of compliance.

Learn more about each accelerator in the sections that follow.

Industry-specific control requirements

Hello! How can I help you?

The framework's [565 control requirements](#) serve as the foundation for the IBM Cloud for Financial Services, and they cover administrative, technical and physical concerns common across the financial services industry. The control requirements were initially based on NIST 800-53 and have been enhanced significantly based on collaboration with major financial institutions around the world. As the regulatory landscape changes, we continue to update the framework based on evolving industry standards and feedback from our partners. In addition, we have [partnered](#) with organizations like the Cloud Security Alliance (CSA) to map the control requirements to the CSA's Cloud Controls Matrix (CCM), a cybersecurity control framework for cloud computing that helps to address third- and fourth-party risk in the cloud.

IBM Cloud provides a rich set of data centers, infrastructure and services which have [evidenced compliance](#) to the control requirements and have been designated as [IBM Cloud for Financial Services Validated](#). This means you can use these components for your financial services workloads knowing that the control requirements are integrated into the technology stack. And keep in mind that all IBM Cloud services are designed with security in mind, and many are certified with other compliance programs, such as ISO, SOC, etc. So, even cloud services that are not yet Financial Services Validated may be considered for use in your solutions depending on your use case, sensitivity of data, etc.

Furthermore, we have a growing partner ecosystem of services and software that have received the Financial Services Validated designation. This means you may use these offerings within your solutions and spend less time and effort vetting third-party risk and compliance.

Guidance and reference architectures

The framework also provides detailed implementation and evidence guidance for each control requirement. The guidance provides the information you need to design, develop, deploy and manage your applications in a way that meets the security and regulatory requirements defined by the control requirements. Along with the extensive [deployment and configuration guidance](#) that takes advantage of a [shared responsibility model](#), three pre-defined reference architectures (shown below) are provided. These architectures demonstrate how to stitch together Financial Services Validated ecosystem components and serve as a secure basis for running your own financial services workloads on IBM Cloud:

- [IBM Cloud® Virtual Private Cloud \(VPC\)](#): This architecture runs on top of [IBM Cloud® Virtual Private Cloud](#) to enable you to establish your own private-cloud-like computing

Hello! How can I help you?

[on IBM Cloud®](#) for compute within your VPC. Like the other reference architectures, it also

describes how to integrate other validated services as part of your solution—for example, [IBM Cloud Hyper Protect Crypto Services](#) to fully manage your encryption keys on industry-leading FIPS 140-2 Level 4-certified hardware.

- **IBM Cloud® Satellite:** This architecture is built using [IBM Cloud Satellite](#) to 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 (such as on-premises). It leverages Red Hat OpenShift on IBM Cloud running within your Satellite environment to host your workloads.
- **IBM Cloud for VMware® Regulated Workloads:** This architecture uses [IBM Cloud for VMware Regulated Workloads](#), 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.

Automated deployable architectures

The framework also provides [Infrastructure as Code \(IaC\)](#) using Terraform—a declarative open-source tool for provisioning and infrastructure orchestration—to automate deployment of the VPC reference architecture on IBM Cloud. This enables you to deploy a reference architecture with greater speed, less risk and reduced cost.

The automation can be run as an [IBM Cloud project](#) to help you build out a secure software development lifecycle (SDLC). When using a project, [Code Risk Analyzer](#) is added to your workflow to provide for code and security scanning. This is an example of “shift left” ([DevSecOps](#)) where security and vulnerability checks are added earlier in the development lifecycle. In this case, Code Risk Analyzer will analyze your Terraform against a set of compliance checks mapped to a subset of control requirements. If any of them fail, your Terraform is not executed. This helps to ensure your deployments are secure by default.

Visit [VPC landing zone deployable architectures](#) to try it out.

Continuous compliance monitoring

Once you’ve deployed your solution, it’s very important to ensure your continued compliance against the control requirements and associated guidance. With [IBM Cloud® Security and](#)

Hello! How can I help you?

action. Unlike Code Risk Analyzer, Security and Compliance Center runs its tests against a live system.

Security and Compliance Center includes a pre-defined [IBM Cloud for Financial Services profile](#) that offers a set of automated tests appropriate for the VPC reference architecture. These tests are mapped to a growing subset of control requirements. While a successful scan does not ensure overall regulatory compliance, it provides a powerful point-in-time statement of your current posture against the control requirements for a specific group of resources against a robust set of baseline tests.

Conclusion

This post shows how the unique industry-specific capabilities of [IBM Cloud for Financial Services](#) are designed to help you reduce risk and accelerate cloud adoption. You've also seen how the resources in the IBM Cloud Framework for Financial Services—control requirements, implementation guidance, reference architectures, automated deployments and continuous compliance monitoring—allow you to make the IBM Cloud for Financial Services work for you as you build your own financial services applications. Our goal for these resources and tools is to free up your resources so that you can focus on core competencies and drive innovation for yourself and your clients.

If you're ready to discuss and align your strategic initiatives, assess your cloud risk or leverage IBM Cloud for Financial Services as a force multiplier, connect with an [IBM Cloud expert](#). In addition, if you represent a financial institution and want to collaborate on reducing the risk of cloud consumption across the financial services industry, we invite you to become a member of the [Financial Services Cloud Community](#).

Author



Tony Erwin

Senior Technical Staff Member



Erick de

Principal Product Manager
Cloud for FS

Hello! How can I help you?

Insights you can't miss. Subscribe to our newsletters.

Go beyond the hype with expert news on AI, quantum computing, cloud, security and much more.

Hello! How can I help you?