**IBM Cloud for Financial ServicesTM**

**FAQ and Field Guide**

# **Introduction**

This Field Guide is a question-and-answer document including contributions from a number of people in support of our IBM Cloud for Financial Services™ sales efforts. It has been produced for the April 7 release of virtual private cloud services. As with the previous versions, it is a living document that will evolve based on our capabilities, clients and market. Your participation in using this guide, engaging our team members shown below, and providing feedback based on your experience in discussions with our prospects and clients is critical to the success of our joint efforts.

# **IBM Cloud Reference FAQ Library:**

* <https://cloud.ibm.com/docs?tab=faqs>

# **IBM Cloud for Financial Services™ Brand Naming Guidelines**

* IBM Cloud for Financial Services™ (no second-reference, short-name)
* IBM Cloud Framework for Financial Services (second-reference, short-name:  Framework for Financial Services\*)
* IBM Cloud for Financial Services™ Validated

# **VMware Offering:**

* The proper naming of our VMware Offering is “IBM Cloud for VMware Regulated Workloads” as it does not carry the FS Cloud nomenclature.

**Guidance**

**IBM Cloud for Financial Services™:**

* In all external collateral / web, etc., state the full name “IBM Cloud for Financial Services™.” Please include trademark symbol.
* When describing IBM Cloud for Financial Services™ in text, do not use term “financial services-ready.” This term is no longer being used. Instead, please use other phrases like: “designed for financial services,” “built for financial services,” “specific to financial institutions,” etc.

**IBM Cloud Framework for Financial Services:**

* “Policy” has been removed from the name. Please do not use IBM Cloud Policy Framework for Financial Services any longer.
* \*Short Name Usage: After the first full usage of the name, the short name can be used for the rest of the text on a web page or in a document.  When using the short name, clearly define that it is referencing the full name before using short name alone i.e., “IBM Cloud Framework for Financial Services (Framework for Financial Services).” Do not include “IBM” in front of ‘Framework.” Use “the Framework for Financial Services.”
* IBM Cloud for Financial Services™ Validated:
  + IBM designates IBM Cloud and ecosystem (ISV, SaaS) services as “IBM Cloud for Financial Services Validated” when the services comply with the IBM Cloud Framework for Financial Services.

Table of Contents

[Introduction 2](#_Toc88037030)

[IBM Cloud Reference FAQ Library: 2](#_Toc88037031)

[IBM Cloud for Financial Services™ Brand Naming Guidelines 2](#_Toc88037032)

[VMware Offering: 2](#_Toc88037033)

[1. What is the IBM Cloud for Financial Services™? 9](#_Toc88037034)

[2. What is IBM Cloud Framework for Financial Services and why is it significant? 10](#_Toc88037035)

[3. What environments will the new release cover? 10](#_Toc88037036)

[4. What offerings or services are available now with IBM Cloud for Financial Services™? 11](#_Toc88037037)

[5. What makes the IBM Cloud for VMware Regulated Workloads different than the standard VMware on IBM Cloud offering? 12](#_Toc88037038)

[6. Are the scopes for controls in various environments (VMware / ROKS) the same or different? 12](#_Toc88037039)

[7. What additional security controls and compliance measures are built into the IBM Cloud for Financial Services™? 13](#_Toc88037040)

[8. What is the IBM Cloud Security and Compliance Center (SCC)? 14](#_Toc88037041)

[9. Does Security and Compliance Center provide for the regulatory compliance in Red Hat (non-VMware) environments? 14](#_Toc88037042)

[10. What is Technology Compliance Advisor (TCA)? 15](#_Toc88037043)

[11. What are new functions / capabilities supporting Developers in the IBM FS Cloud™? 15](#_Toc88037044)

[12. Are there additional terms and conditions required for Client Banks to use IBM Cloud services with IBM Cloud for Financial Services™? 16](#_Toc88037045)

[13. How are backups of the database managed? Where is the database backup stored? Can the database backup be exported? Is the database backup encrypted? Can the database backup be automated? 16](#_Toc88037046)

[14. Is ongoing compliance monitoring (including changes) based on an ongoing services engagement from IBM Services? Or is it something clients are intended to implement in e.g., Caveonix, SCC, etc.? 17](#_Toc88037047)

[15. Please describe cyber and technology control transparency and reporting for IBM owned controls relating to xAAS services and systems supporting the hosted client bank applications. 17](#_Toc88037048)

[16. If a client is using another cloud, the below-the-line controls discussion and review may have already taken place. How can we assist given that the existing cloud provider may have performed the security / compliance process? 19](#_Toc88037049)

[17. How is the end-to-end environment managed from a Regulatory Compliance standpoint? 20](#_Toc88037050)

[18. What is a Cloud Control Analysis (formerly known as Control Mapping)? 20](#_Toc88037051)

[19. What is the scope of regulators included with IBM's financial services spectrum? 22](#_Toc88037052)

[20. Are Cloud Service Provider (IBM) feature set enhancements subject to client bank approval and release control? 22](#_Toc88037053)

[21. Are there specific geographical considerations, e.g., GDPR, that may need to be taken into consideration? 22](#_Toc88037054)

[22. What other regulatory approvals / compliance are we seeking? 25](#_Toc88037055)

[23. How can someone gain visibility to security posture and threats? 25](#_Toc88037056)

[24. How can someone ensure their resources are configured securely? 26](#_Toc88037057)

[25. How does IBM propose to implement a shared responsibility model reporting on compliance of IBM controls and enabling a client bank control reporting for its owned controls? 26](#_Toc88037058)

[26. Will IBM still comply with existing industry standards? 28](#_Toc88037059)

[27. How are controls related to managed services and APIs integrated into the client bank preventative and detective control operating effectiveness reporting? 29](#_Toc88037060)

[28. Are regulators endorsing the IBM Cloud for Financial Services™? 29](#_Toc88037061)

[29. Can IBM provide an audit report on our operating environment (SOC2 type)? 29](#_Toc88037062)

[30. Does IBM FS Cloud support least privilege policies for applications accessing cloud resources? 29](#_Toc88037063)

[31. Does IBM FS Cloud support identification of anomalous user activity and have ability to send alerts to client's SIEM? 30](#_Toc88037064)

[32. Does IBM FS Cloud support logs only being accessible to users with a legitimate business requirement and protecting logs from unauthorized modification or deletion? 30](#_Toc88037065)

[33. What separation is suggested for different SDLC environments, such as Dev, SI, Prod? How is this separation achieved? 33](#_Toc88037066)

[34. How does IBM Cloud for Financial Services integrate with client's Global Authorization solution for authentication and multi-factor authentication (MFA)? 35](#_Toc88037067)

[35. Does IBM Cloud for Financial Services support data encryption keys being rotated on at least an annual basis? 35](#_Toc88037068)

[36. Does IBM Cloud for Financial Services support client data processed or stored in the cloud environment must be monitored and subject to Data Loss Prevention (DLP) scans with applicable controls? 37](#_Toc88037069)

[37. Does IBM Cloud for Financial Services support stateful packet inspection be required for inbound -outbound network internet traffic for public IaaS & PaaS environments and packet inspection for private cloud done at core network perimeter? 37](#_Toc88037070)

[38. Can IBM Cloud for Financial Services resources be configured to prevent direct internet connections unless required for a defined business purpose? 39](#_Toc88037071)

[39. Can all IBM Cloud for Financial Services data be encrypted in transit and at rest? 41](#_Toc88037072)

[40. Can a client restrict what cloud services are available to developers in the different environments? How? 41](#_Toc88037073)

[41. Can a client grant temporary (time-based) access to administrative permissions in higher environments (SI/Prod)? 42](#_Toc88037074)

[42. Can traffic at public internet boundaries be monitored and with all known malicious IP addresses blocked? 43](#_Toc88037075)

[43. Can public IaaS and PaaS environments have an automated Intrusion Detection / Prevention System (IDS/IPS) in place for all inbound and outbound internet traffic? 43](#_Toc88037076)

[44. Can public endpoints be protected using a combination of a content delivery network (CDN) and a web application firewall? 44](#_Toc88037077)

[45. Are insecure and unencrypted protocols blocked in all cloud environments? 45](#_Toc88037078)

[46. Is access to IBM’s resources strictly controlled to ensure only those with a required need to access such services are permitted and that only the appropriate level of access is allowed? 45](#_Toc88037079)

[47. What cloud audit log information from IaaS and PaaS environments is able to be collected and integrated with the client SIEM tool? 47](#_Toc88037080)

[48. Can both environments exist at the same time (VMware and non-VMware)? 47](#_Toc88037081)

[49. How will a bank need to change its operating model to enable the IBM Cloud for Financial Services™ e.g., organizational maturity level within a cloud adoption framework? 47](#_Toc88037082)

[50. When will cloud-native services be available? 48](#_Toc88037083)

[51. What is the roadmap for IBM PaaS and SaaS services to be available on IBM Cloud for Financial Services™? For example, when will Watson APIs, managed API services be available? 48](#_Toc88037084)

[52. Will IBM Cloud for Financial Services™ support IBM Cloud Satellite for management of OpenShift? 48](#_Toc88037085)

[53. Are there technology roadmaps for PaaS and SaaS that can be shared with client banks to aid joint development of controls and limit duplication? 48](#_Toc88037086)

[SOLUTIONING 49](#_Toc88037087)

[54. How is capacity and automation (autoscaling) configured and reported via control interfaces into a client bank (development, security, and operations)? 49](#_Toc88037088)

[55. What level of management of the infrastructure is provided? Are OS, patching, and high availability (HA) managed across multiple data centers? Is the scaling managed / automated? 50](#_Toc88037089)

[56. What is the shared application identity model used across application services? 51](#_Toc88037090)

[57. How does the IBM Cloud for Financial Services control the geographic deployment location the scheduler runs in? 52](#_Toc88037091)

[58. What is required to develop, deploy, and maintain applications consistently across any infrastructure? 53](#_Toc88037092)

[59. What is required to consistently ensure security across hybrid, multicloud environments? 53](#_Toc88037093)

[60. How is control compliance CI/CD [continuous integration (CI) and continuous delivery (CD)] reported in IBM Cloud for Financial Services? 55](#_Toc88037094)

[61. Does IBM outsource any part of its cloud operations? 55](#_Toc88037095)

[62. What type of skills do I need to build to operate IBM Cloud for Financial Services? 55](#_Toc88037096)

[MARKETING 55](#_Toc88037097)

[63. How does the IBM Cloud for Financial Services™ help banks and financial institutions accelerate compliance efforts while reducing costs and risk to maintain regulatory compliance? 55](#_Toc88037098)

[64. What value does the IBM Cloud for Financial Services™ bring to financial institutions and their ISV channels? 57](#_Toc88037099)

[65. How can the IBM Cloud for Financial Services™ help banks manage the stream of regulatory requirements and updates for bank workloads or SaaS applications? 58](#_Toc88037100)

[66. What are the primary value propositions of the IBM Cloud for Financial Services? 59](#_Toc88037101)

[67. What makes IBM the right cloud provider to take on this endeavor? 62](#_Toc88037102)

[68. What is the business case for IBM Cloud for Financial Services™? 64](#_Toc88037103)

[69. What costs can client banks avoid by using the controls now provided out of the box? 69](#_Toc88037104)

[70. What is the contracting process for IBM Cloud for Financial Services™? 71](#_Toc88037105)

[71. Does charge for ingress and replication within IBM Cloud environments? 71](#_Toc88037106)

[72. Are there example playbook / sales cycle approach for solutioning IBM Cloud for Financial Services™ for Banks and ISVs / SaaS? 72](#_Toc88037107)

[73. How do I help client banks engage around the Framework for Financial Services or plan to use IBM Cloud for Financial Services™? 72](#_Toc88037108)

[74. What is the IBM Research Cloud Innovation Lab? 73](#_Toc88037109)

[75. How do reseller partners participate in IBM Cloud for VMware Regulated Workloads? 73](#_Toc88037110)

[76. Are Global System Integrators (GSI) participating in IBM Cloud for VMware Regulated Workloads? 73](#_Toc88037111)

[77. What ISV and SaaS providers intend to onboard their offerings to the IBM Cloud for Financial Services™? 73](#_Toc88037112)

[78. Can we consider onboarding the ISVs and SaaS providers that my financial institution client uses or is interested in? 75](#_Toc88037113)

[79. How can ISVs and SaaS providers participate in the IBM Cloud for Financial Services™? 75](#_Toc88037114)

[80. What technical assistance is provided to ISVs and SaaS providers? 75](#_Toc88037115)

[81. What is the IBM Financial Services Cloud Council? 76](#_Toc88037116)

[82. Are there other financial institutions who have agreed to adopt the IBM Cloud for Financial Services™? 76](#_Toc88037117)

[83. What are IBM’s experiences / assets / accelerators in this space? 77](#_Toc88037118)

[84. What are the Service Level Agreements (SLA) for FS Cloud? 78](#_Toc88037119)

[Appendix A: Acronyms and Definitions 79](#_Toc88037120)

|  |
| --- |
| **Understanding** |
|  |
| **What is the IBM Cloud for Financial Services™?** |
| The IBM Cloud for Financial Services™ is a solution platform and ecosystem program for financial institutions and their technology providers. IBM Cloud for Financial Services is designed to enable the use of mission-critical, data-sensitive workloads in the public cloud. It provides Confidential Computing and KYOK for technology-assured safeguarding of data, pre-configured controls built into standard cloud services to reduce compliance risk and costs and features a growing ecosystem of 80+ ISV and SaaS provider partners.  The IBM Cloud for Financial Services™ comprises IBM Cloud services and independent software vendor (ISV), SaaS and financial institution applications that operate in standard IBM Cloud Multi-Zone Regions (MZRs) and comply with IBM Cloud Framework for Financial Services. The cloud services can be supported by separately available and purchased consulting services from IBM Promontory, IBM Security Services, IBM Global Services, and IBM business partner service providers.  Client solutioning may start before GA with foundational cloud services denoted in the offering description, while controls deployment and validation, and regulatory partners are finalized.  The IBM Cloud Framework for Financial Services (Framework for Financial Services) establishes the controls, controls guidance and architecture requirements for compliance for the IBM Cloud for Financial Services™. For VMware Regulated Workloads, deployment guidance and a controls implementation overview for ISV and SaaS providers specifies control objectives and implementation and evidence guidance for the provider partner, as well as specifies what portion of the control is satisfied by IBM Cloud and what portion is the responsibility of the provider. This documentation is available via PartnerWorld (see link below) and is complimentary to ISVs / SaaS providers who have signed a memorandum of understanding to onboard to the IBM Cloud for Financial Services™.  For virtual private cloud services, deployment guidance documentation may be requested.  **IBM Cloud for VMware Regulated Workloads** is an offering validated for use with IBM Cloud for Financial Services™. VMware Regulated Workloads is a prescriptive reference-architecture solution designed for security and network and compute isolation. The offering provides the highest level of security and compliance needed for regulated workloads.  Designed to enable a zero-trust model, the reference architecture offers clients across industries a strategic cloud approach to securely extend and scale their VMware IT operations to IBM Cloud and to be compliance ready. |
| **What is IBM Cloud Framework for Financial Services and why is it significant?** |
| The IBM Cloud Framework for Financial Services is an industry-informed set of controls and operations that mitigates systemic risk in using public cloud for sensitive-data banking workloads. IBM collaborated in the industry with Bank of America and others and applied regulatory expertise from IBM Promontory to establish the Framework for the industry. The common controls criteria are applied to IBM Cloud services and the ecosystem of ISV, SaaS and Fintec provider partners in our program, and enables the level of transparency, compliance and security required for all parties – banks, cloud and ecosystem providers - to operate securely and confidently. The IBM Financial Services Cloud Council, comprised of CxOs across technology, information security and risk from leading worldwide financial institutions, will help maintain and evolve the Framework for cybersecurity and regulatory requirements for the industry.  The Framework addresses 280 controls across 21 controls families, and uses common controls language from US NIST 800-53, with 54 controls written with IBM financial services guidance. IBM builds the controls into IBM Cloud services and validates controls into ecosystem provider offerings. These pre-configured controls enable continuous compliance, accelerate workload transformation and reduce compliance costs. |
| **What environments will the new release cover?** |
| Virtual Private Cloud services with IBM Cloud for Financial Services were released 1Q.2021 and are available in the IBM Cloud Catalog with a Financial Services Validated designation. These services include:   * Red Hat OpenShift on IBM Cloud * IBM Virtual Server for Virtual Private Cloud * IBM Cloud Object Storage * IBM Block Storage for Virtual Private Cloud * Virtual Private Cloud services |
| **What offerings or services are available now with IBM Cloud for Financial Services™?** |
| IBM Cloud for Financial Services Validated offerings include Virtual Private Cloud services and IBM Cloud for VMware Regulated Workloads.  Services designated as IBM Cloud for Financial Services Validated can be found in the IBM Cloud Catalog ([cloud.ibm.com](http://cloud.ibm.com/)) by searching for or using the compliance filter for “Financial Services Validated.”  The number and type of services vary depending on the platform. Information is shown below for IBM Cloud for VMware regulated Workloads and for IBM Cloud Virtual Private Cloud.  **IBM Cloud Virtual Private Cloud services:**   * IBM Access Management (IAM) * IBM Activity Tracker (via COS) * IBM Cloud App ID * IBM Cloud Container Registry * RedHat OpenShift on IBM Cloud (ROKS) * IBM Cloud Object Storage (COS) * IBM Event Streams for IBM Cloud * Business Support Services (BSS) * Global Catalog * IBM Cloud CLI * IBM Cloud Hyper Protect Crypto Services (HPCS) * IBM Cloud Direct Link Dedicated (2.0) (networking) * IBM Cloud DNS Services (Domain Name Service) * IBM Cloud Transit Gateway * IBM Cloud Virtual Private Cloud - Load Balancer (Gen 2) * IBM Cloud Virtual Private Cloud - VPN (Gen 2) * IBM Cloud Service Endpoint (CSE) * IBM Cloud Virtual Private Endpoint for VPC * IBM Cloud Virtual Private Cloud (Gen 2) * IBM Cloud Virtual Server for Virtual Private Cloud (Gen 2), including:   + IBM Cloud Virtual Private Cloud - Dedicated Hosts   + IBM Cloud Virtual Private Cloud - Flow Log   + IBM Cloud Virtual Private Cloud - Auto Scale   + IBM Cloud Block Storage for Virtual Private Cloud   **Advisory and Technology Services**   * IBM Garage for Cloud * IBM Cloud Engagement Hub * IBM Cloud Solutioning Center * IBM Developer Advocacy (patterns) * IBM GBS * IBM GTS * IBM Promontory * IBM Security Services * IBM business partners (roadmap)   For additional information:   * Cloud Service Catalog, search for “Validated Services” at: <https://cloud.ibm.com/catalog#services> * Cloud Software Catalog: <https://cloud.ibm.com/catalog#software> * Cloud Consulting Catalog: <https://cloud.ibm.com/catalog#consulting> |
| * IBM Cloud Catalog: <https://cloud.ibm.com/infrastructure/vmware-solutions/console/ordernew/dedicated/vcs_nsx_t> * [IBM Cloud for Financial Services™](https://www.ibm.com/cloud/financial-services): <https://www.ibm.com/cloud/financial-services> |
|  |
| **What makes the IBM Cloud for VMware Regulated Workloads different than the standard VMware on IBM Cloud offering?** |
| IBM Cloud for VMware Regulated Workloads is a more robust, prescriptive architecture compared to the standard VMware on IBM Cloud offerings. The Regulated Workloads solution is designed for worker and management node isolation and starts at 10 nodes and three individual clusters (edge, management, worker) to meet stringent compliance need. The standard VMware on IBM Cloud offering starts at three nodes and is designed for more general, non-regulated workload use cases. |
| **Are the scopes for controls in various environments (VMware / ROKS) the same or different?** |
| The scopes of controls or control objectives of FS Cloud in VMWare / ROKS environments are the same, meaning that all of the IBM Cloud Framework for Financial Services control objectives apply to IBM Cloud for VMware Regulated Workloads and all of the Framework control objectives apply to an FS Cloud cloud-native environment. The actual mitigations employed to achieve the control objectives within VMware and cloud native environments are considerably different. For example, the security, compliance and backup disaster recovery (DR) services are handled differently for each environment to meet the same set of controls. |
| **What additional security controls and compliance measures are built into the IBM Cloud for Financial Services™?** |
| The cloud services that make up the IBM Cloud for Financial Services adhere to foundation of global and industry standards such as SOC 2 Type 2, PCI-DSS, ISO, and more. IBM Cloud Framework for Financial Services includes 280 controls across 21 control categories including system security, integrity resiliency, and other risk management matters.  IBM aligned the controls to the United States National Institute of Standards and Technology (NIST) Special Publication 800-53 industry standard framework to drive rapid understanding and implementation.  The controls are financial services industry-informed to meet specific implementation standards.    For additional information on the underlying compliance posture of the cloud services that make up the IBM Cloud for Financial Services:   * IBM Cloud Compliance: [www.ibm.cloud/compliance](http://www.ibm.cloud/compliance) * IBM public cloud compliance posture & roadmap dashboard (commercial): <https://www.ibm.com/w3-techblog/compliance> |
| **What is the IBM Cloud Security and Compliance Center (SCC)?** |
| IBM Cloud Security and Compliance Center is a security and compliance dashboard included with an IBM public cloud account. Clients can define controls, assess posture, monitor security and compliance, remediate issues and collect audit evidence. IBM Cloud Security and Compliance Center is a key to achieving continuous security and compliance, allowing clients to assess the security and compliance posture of their workloads with IBM Cloud for Financial Services. Additionally, for multicloud deployment models, clients can use SCC to manage their own controls or general profiles in multiple cloud service providers (IBM Cloud for Financial Services controls are specific to IBM public cloud and, in 2H.2021, to on-premises deployments using IBM Cloud Satellite).   * Getting started with Security and Compliance Center: <https://cloud.ibm.com/docs/security-compliance?topic=security-compliance-getting-started> |
| **Does Security and Compliance Center provide for the regulatory compliance in Red Hat (non-VMware) environments?** |
| Yes. IBM Cloud Security and Compliance Center provides compliance management and enforcement for all IBM cloud services except IBM Cloud for VMware Regulated Workloads, which uses Caveonix RiskForesight for its compliance management functions.  Clients can use the Security and Compliance Center to monitor their security and compliance posture in the following environments:   * IBM Cloud * Amazon Web Services * Google Cloud Platform * Microsoft Azure * On-premises   Clients can use the Security and Compliance Center to scan and monitor their resources that pertain to the following services:   |  |  | | --- | --- | | * Activity Tracker with LogDNA | * IBM Cloudant | | * Block Storage | * IBM Cloud VPC | | * Certificate Manager | * Cloud Internet Services (CIS) | | * Cloud Databases | * Key Protect | | * Cloud Identity and Access Management | * Object Storage | | * Container Registry | * Security Advisor | | * Continuous Delivery |  |   For additional information:  Global and industry certifications:  <https://www.ibm.com/cloud/compliance> |
| **What is Technology Compliance Advisor (TCA)?** |
| Technology Compliance Advisor (TCA) is a solution to manage an organization's control environment and is used in IBM Security Services advisory service engagements.  TCA integrates with IBM Promontory’s regulatory obligation library and maps a client's external regulatory obligations to control objectives from NIST, ISO, CSA and more and to the client’s control objectives and specific controls.  The service provides impact tracing and change management of regulatory changes to the client’s policies, control objectives, and controls. TCA and the service integrate with IBM OpenPages RegTech software to classify controls by business unit, business process, product / service offerings or risk domain (e.g., cloud). |
| **What are new functions / capabilities supporting Developers in the IBM FS Cloud™?** |
| With the release of the Virtual Private Cloud services for IBM Cloud for Financial Services, banks and their technology partners can now build applications with Red Hat OpenShift, migrate virtual machine workloads, and establish compliance profiles across their workloads– to help achieve continuous compliance. Financial services institutions can now accelerate their cloud journeys with IBM Cloud for Financial Services’ built-in security and compliance controls for cloud-native and VMware workloads.    IBM Cloud for Financial Services is built on IBM Cloud, the industry’s most secure and open cloud for business, which uses Red Hat OpenShift as its primary Kubernetes environment to manage containerized software across the enterprise, and includes more than 200 in-scope, API-driven, cloud-native PaaS services to create new and enhanced cloud-native apps. Developer and ecosystem partners can build and modernize in a secure environment to drive innovation for today’s modern banking client. Roadmap directions for developer productivity include automating DevSecOps pipelines with ongoing security and compliance profile enforcement via the integration of IBM Code Risk Analyzer and IBM Cloud Security and Compliance Center and enabling automated secure landing zones for ISV and SaaS ecosystem partners.  The IBM Developer Advocacy team provides a developer pattern and technical blog guiding the use of Red Hat OpenShift on IBM Cloud (ROKS) in an IBM Cloud for Financial Services build environment; see <https://developer.ibm.com>.  Solution Tutorials: IBM provides training on how to build, deploy, and scale real-world solutions on IBM Cloud. Solution tutorials provide step-by-step instructions on how to use IBM Cloud to implement common patterns based on best practices and proven technologies. |
| **Are there additional terms and conditions required for Client Banks to use IBM Cloud services with IBM Cloud for Financial Services™?** |
| No. Use the standard cloud services agreement (CSA) with services for IBM Cloud for Financial Services. IBM Cloud for Financial Services does not require nor provide additional terms beyond the standard CSA.  For additional information:   * The Cloud Service Agreement: <https://www.ibm.com/support/customer/csol/terms/> |
| **How are backups of the database managed? Where is the database backup stored? Can the database backup be exported? Is the database backup encrypted? Can the database backup be automated?** |
| For VMware Regulated Workloads runtimes, clients can manage backup and recovery of databases using the applicable database vendor guidance.  For additional information:   * VMware FAQ VMware vSphere Storage APIs – Data Protection: <https://kb.vmware.com/s/article/1021175> * Backup & Recovery for IBM Cloud, Storage and Services: <https://www.veeam.com/ibm-cloud-storage-services-solutions.html?ad=in-text-link> * Veeam, How Back Up Works (v11): <https://helpcenter.veeam.com/docs/backup/vsphere/backup_hiw.html?ver=110> * (Internal) Veeam on bare metal server: <https://cloud.ibm.com/docs/vmwaresolutions?topic=vmwaresolutions-veeam-bms-archi-overview> * (Internal) Getting started with VMware Solutions: https://cloud.ibm.com/docs/vmwaresolutions?topic=vmwaresolutions-getting-started |
| **Is ongoing compliance monitoring (including changes) based on an ongoing services engagement from IBM Services? Or is it something clients are intended to implement in e.g., Caveonix, SCC, etc.?** |
| On-going monitoring of controls from Security & Compliance Center (SCC) will be available for clients use, but it is not a managed service that IBM performs. Typically, the client’s Security Operation Center (SOC) or Compliance Monitoring team will be using the SCC monitoring capabilities.  IBM will provide documentation to changes in the underling IaaS and relevant IBM managed components for client integration into relevant security documentation and procedures  IBM Security and Promontory have partnered to offer Technology Compliance Advisor (TCA) which ensures alignment and ongoing support for clients who want to ensure regulatory compliance with new and changing regulations in the ever-revolving regulatory landscape. |
| **Please describe cyber and technology control transparency and reporting for IBM owned controls relating to xAAS services and systems supporting the hosted client bank applications.** |
| Each IBM service designated as IBM Cloud for Financial Services Validated goes through the IBM Public Cloud Compliance team assessment and testing of the Framework controls implementation. If a control is determined to not be fully implemented, an exception process is initiated, and the issue is tracked to remediation.  **Configuration Governance**  Clients can create rules to standardize resource configuration across their accounts. Configuration rules are guardrails for how resources can be provisioned and configured. By attaching the rules to a scope, clients can monitor and enforce rules in only the areas that they want to target. Through rule enforcement and customized defaults, clients can code configurations with confidence to follow the guidelines that they put in place - significantly decreasing the likelihood of misconfiguration-related security issues.  Using the Enterprise capability of IBM Cloud, lines of business or application instances can be segregated using separate cloud accounts, as shown below in the four-tier enterprise hierarchy.  The billing will be rolled-up to the Enterprise level giving a plan view with no instance level detail. Access to an individual Account will provide the instance level detail. Billing usage and discounts is applied at the Enterprise level based on aggregated usage volumes..  **Security Insights**  With Security Insights, clients can continuously monitor and analyze IBM Cloud resources and applications for potential risks. With Security Insights, clients get access to threat detection, security risk prevention, and suggested remediation steps that can help to mitigate issues found, send customized alert notifications, and can give them a more comprehensive understanding of their current security status. Note: Security Insights is available for IBM Cloud only.  For additional information:   * Security and Compliance Center: <https://cloud.ibm.com/docs/security-compliance?topic=security-compliance-overview> * Apply end to end security to a cloud application: <https://cloud.ibm.com/docs/solution-tutorials?topic=solution-tutorials-cloud-e2e-security> * Caveonix RiskForesight: <https://www.caveonix.com/platform/riskforesight> * Security Insights: <https://cloud.ibm.com/docs/security-advisor?topic=security-advisor-insights>  1. **If a client is using another cloud, the below-the-line controls discussion and review may have already taken place. How can we assist given that the existing cloud provider may have performed the security / compliance process?** |
| It’s important to understand the question and remove any assumptions that could cause confusion by clarifying terms and phrases such as above-the-line and “below-the-line.” The line reference is the “Line of Shared Responsibility.”  Cloud service providers adhere to a shared security responsibility model which means the client’s security team maintains some responsibilities for security as applications, data, containers, and workloads are moved to the cloud. While the provider takes some responsibility, the client – a bank as an example – is also responsible. Defining the line demarcating which are whose responsibilities is critical for identifying and mitigating risks associated with managing public, hybrid, and multi-cloud environments.  It’s important to know that the delineation of shared responsibility is not static and may vary by provider and service type. In a traditional data center model, clients are responsible for security across the entire operating environment, including applications, physical servers, user controls, and physical facilities. In a cloud environment, the provider – IBM in this case – can reduce the security management burden from clients by taking responsibility for some or many operational activities, including security. In the shared responsibility model, ownership of which domain and or service must be clearly defined. It is then expected that each party will be responsible for controlling the assets, processes, and functions they own. Working together with our clients to define and share portions of the security requirements, will provide a secure environment with reduced operational overhead. |
| In our experience, other Cloud Service Providers (CSP) typically provide SOC 2 reports as evidence of their below-the-line controls. However, it is not uncommon for other CSPs to use a different set of controls for below-the-line items. IBM Cloud for Financial Services™ uses the same control foundation for above-the-line and below-the-line components.  It is recommended that a full review be performed unless a qualified certification can be shown to have been performed previously by an acceptable party.  IBM cannot assume a bank has performed an acceptable below-the-line certification from both an information security and compliance perspective. A bank may have only assessed data security and encryption (above-the-line). The below-the-line requirements may be touched, but where IBM differentiates itself is by continuous governance with the drift of controls and policies. This is where this bank was highly interested and separated us from AWS. AWS claims SOC and PCI compliance which is static - if the policies drift and change, the question that was raised is how does a cloud provider handle and adapt to the changes? |
| **How is the end-to-end environment managed from a Regulatory Compliance standpoint?** |
| The Framework for Financial Services Base Controls (NIST with IBM financial services guidance) are a comprehensive set of controls that align well in enabling the IBM Cloud for Financial Services to support clients in meeting their regulatory obligations. The IBM Cloud services are validated against these controls and ISV / SaaS providers also go through a validation process to confirm adoption of the controls. The environment is monitored using Security and Compliance Center which displays deviation from controls.  For additional information:   * Apply end to end security to a cloud application: <https://cloud.ibm.com/docs/solution-tutorials?topic=solution-tutorials-cloud-e2e-security> * Architecture overview: <https://cloud.ibm.com/docs/vmwaresolutions?topic=vmwaresolutions-vrw-archi-overview> |
| **What is a Cloud Control Analysis (formerly known as Control Mapping)?** |
| Cloud Control Analysis / Control Assessment Services / Control Mapping Service is a client facing service that is used during the sales cycle to demonstrate the value of IBM Cloud for Financial ServicesTM. This process requires the client to share their cloud control set which is mapped to the IBM Cloud Framework for Financial Services control set resulting in establishing that Framework controls meet or exceed client control requirements.  Control Analysis compares and analyzes controls in the IBM Framework for Financial Services and those a client uses in their environment. This analysis provides a view on the coverage of IBM’s controls (the number and or percentage) to the client’s controls.  An example Control Analysis summary may include the following findings:   * 26 client Controls do not map to the Framework for Financial Services   + 14 controls can be addressed by supplemental guidance related controls   + 12 controls are not technologically related but instead related to organization, process, documentational.  |  |  |  | | --- | --- | --- | | **NIST800-53r4**  **CONTROL REFERENCE** | **CONTROL TITLE** | **MAPPING COMMENTS** | | AU-15 | ALTERNATE AUDIT CAPABILITY | Alternate audit process will need to be defined by BANK and IBM will work with BANK and provide the necessary information to fulfill the requirements | | AU-16 | CROSS-ORGANIZATIONAL AUDITING | Cross organization audit process and scope shall be defined by BANK and IBM will work with BANK and provide information needs to fulfill the requirements |   The objective of the analysis is to provide:   * The bank with an understanding of IBM Framework for Financial Services alignment to existing bank controls * IBM with an understanding of how well the Framework for Financial Services aligns to:   + a specific bank   + broad banking industry requirements as evidenced by comparison to a range of banks included in Control analysis engagements |
| **What is the scope of regulators included with IBM's financial services spectrum?** |
| Promontory has assessed the alignment of the IBM Cloud Framework for Financial Services (Framework) controls to EBA guidelines and key financial regulations in France, UK, Germany, Australia, Brazil, Canada, United States and Japan.  This initial assessment by Promontory was focused on the Framework Base controls as documented to determine, from the perspective of a cloud service provider, how they align with the regulations to help FI clients meet their obligations. The IBM Framework controls are not designed to map one to one to the regulatory obligations of a financial institution.  IBM and Promontory have deep involvement in banking and the regulatory industry. We consult on business, legal, compliance, operations, and technical areas for the largest, most complex financial services companies. Promontory has expertise and ongoing coverage of regulatory activities across:   * 24 jurisdictions (23 countries plus the European Union) * 75 regulatory and standards issuing bodies   For additional information:   * Promontory regulatory advisory: <https://www.promontory.com> |
| **Are Cloud Service Provider (IBM) feature set enhancements subject to client bank approval and release control?** |
| At this time, feature set enhancements, including controls, follow an established change management process. Clients will be informed but are not part of the approval process, at this time.  For IAAS, they are certified as additional features in Kubernetes and VMware at client’s discretion post setup. |
| **Are there specific geographical considerations, e.g., GDPR, that may need to be taken into consideration?** |
| Yes. There are several considerations at the state, country, region levels that must be addressed. Our IBM Cloud for Financial Services™ safeguards our clients' most valuable assets by providing market-leading data protection, privacy, and visibility into where all data is at all times. It's also supported by IBM Security, designed to support government and industry compliance, and uses the same state-of-the-art cryptographic technology that financial institutions rely on.  The IBM Cloud for VMware Regulated Workloads offerings operate in worldwide multi-zone regions with the Framework. The offering may be paired with cloud compliance offerings such as EU Cloud.  The IBM Cloud Framework for Financial Services applies Base Controls that have applicability in other countries. As anchor clients are secured in other regions, any impact of geo specific regulations on the Framework controls will be addressed.  We provide infrastructure and expertise designed to help our clients achieve compliance with industry standards and government regulations. We support a broad range of global, regional, and industry regulatory requirements including  [International Organization for Standardization (ISO),](https://www.iso.org/home.html)  Payment Card Industry (PCI), [Health Insurance Portability and Accountability Act (HIPAA), General Data Protection Regulation (GDPR), and](https://www.cdc.gov/phlp/publications/topic/hipaa.html)  [Social Expenditure Database (SOCx).](https://www.cdc.gov/phlp/publications/topic/hipaa.html)  Additionally, clients are able to comply with data sovereignty regulations across 35 worldwide VMware data centers. IBM Cloud for Financial Services™ enforces compliance requirements through geofencing to assure audit readiness. As background, data sovereignty requires that the personal data of citizens of a specific country remain within that country's borders, e.g., personal data of German citizens must be stored within German geographic boundaries.  Examples of regional regulators and standards in Europe and United Kingdom include:   * BaFin (Germany): BaFin, formally known as the German Federal Financial Supervisory Authority, oversees all financial services firms in Germany. BaFin has published a specification for the regulatory framework for cloud computing services provided to financial services firms. * C5 (Germany): The Cloud Computing Compliance Controls Catalog (C5), introduced by the German Federal Office for Information Security (BSI), is a cloud-specific attestation scheme. This scheme outlines the requirements cloud service providers must meet in order to ensure a minimum-security level for their cloud services. C5 elevates the demands on cloud providers by combining existing security standards such as ISO 27001, with additional requirements for increased transparency in data processing. * European Banking Authority - EBA (EU): As part of its mission to establish consistent, efficient and effective supervisory practices across the EU and ensure uniform application of Union law, the European Banking Authority (EBA) issues regulatory guidelines and recommendations in its fields of competence. * ENISA IAF (EU): The European Union Agency for Network and Information Security (ENISA) issued the Information Assurance Framework (IAF), a set of assurance criteria designed to assess the risk of adopting cloud services, comparing different cloud provider offers, obtaining assurance from the selected cloud providers, and reducing their assurance burden. * ENS (Spain): The National Security Framework of Spain (ENS) is a legal decree that develops provisions about security and applies them to all public administrations in Spain. The ENS establishes the security policy for eGovernment services. It establishes the basic principles and minimum requirements to enable adequate protection of information to be followed by all public administrations. * EU Model Clauses: EU Model Clauses are available to controllers and processors of EU citizens' Personally Identifiable Information (PII). These clauses obligate non-EU companies to follow the laws and practices mandated by the EU Data Protection Directive in all global locations. The clauses provide enforcement rights and assurance to companies that hold EU PII that providers located outside of the EU will process data only in accordance with their instructions and in conformance with EU laws. In May 2018, the EU Data Protection Directive was replaced by the General Data Protection Regulation (GDPR). * EU-US Privacy Shield: The EU-US and Swiss-US Privacy Shield Frameworks were designed by the US Department of Commerce and the European Commission and Swiss Administration. These frameworks provide companies on both sides of the Atlantic with a mechanism that helps them comply with data-protection requirements when they transfer personal data from the European Union (EU) and Switzerland to the United States in support of transatlantic commerce. * GDPR (EU): As part of the European Union's General Data Protection Regulation (GDPR), IBM is enhancing its ongoing commitment to privacy by design. IBM is working to embed data protection principles even more deeply into its business processes. This work also strengthens existing controls to limit access to personal data, including mobile applications that rely on default settings to prevent sharing of personal data. * G-Cloud (UK): The government of the United Kingdom created the G-Cloud framework to enable a faster and less expensive process for UK government organizations to enter into procurement contracts with cloud providers. G-Cloud services are divided into three categories: cloud hosting, cloud software, and cloud support. * Hébergeurs de Données de Santé - HDS; Health Data Hosting (France): Hébergeurs de Données de Santé (HDS) is designed to describe the conditions under which personal health data initially collected in France must be protected. Data hosting must include security controls commensurate with the critical nature of the data. Any individual or legal person who hosts personal health data collected in France must be approved or certified for this purpose * IT-Grundschutz (Germany): The aim of IT-Grundschutz is to achieve an appropriate security level for all types of information in an organization. IT-Grundschutz uses a holistic approach to this process, and provides guidance for the application of technical, organizational, personnel and infrastructural safeguards. * NIS Directive (EU): The Network and Information Systems (NIS) Directive (EU 2016/1148) is the first cybersecurity law to cover the entire the European Union and is intended to boost the overall cybersecurity level for critical infrastructure in the EU.   IBM maintains standard technical and organizational measures appropriate and proportionate to manage the risks posed to the security of network and information systems. This includes a security monitoring program and a global incident response process to respond to cybersecurity threats and attacks. In addition, IBM utilizes a combination of online training, educational tools, videos and other awareness initiatives to foster a culture of security awareness and responsibility among its workforce. More information on these technical and organizational measures is available in IBM certifications and audit reports such as ISO 27001 and SOC 2.  For additional information:   * [Techblog - Compliance](file:///C:\Users\brettsibmmacair\Documents\00%20-%20Cloud%20Engagement%20Hub\00%20-%20Sales%20Support\00%20-%20FAQ%20and%20Field%20Guide%20for%20IBM%20Cloud%20for%20Financial%20Services\00%20-%202021-1Q%20FS%20Field%20Guide\Draft%20versions\Techblog%20-%20Compliance): <https://www.ibm.com/w3-techblog/compliance/> * [Cloud Compliance Regional](https://www.ibm.com/cloud/compliance/regional): <https://www.ibm.com/cloud/compliance/regional> |
|  |
| **What other regulatory approvals / compliance are we seeking?** |
| IBM and Promontory in conjunction with the IBM FS Cloud offering team have a deep understanding of the financial services and regulatory industry and are asked, when appropriate, to participate and or comment on future or pending regulation. An example of this is our recent participation in contributing to the EBA revised Guidelines on outsourcing arrangements released earlier in 2020. |
| **How can someone gain visibility to security posture and threats?** |
| Various different sources can be used for security posture and threats including public forms also membership-based forums including FS-ISAC.   * [VMware Solutions Architecture Overview](https://cloud.ibm.com/docs/vmwaresolutions?topic=vmwaresolutions-vrw-archi-overview): <https://cloud.ibm.com/docs/vmwaresolutions?topic=vmwaresolutions-vrw-archi-overview> * Caveonix Risk Foresight: <https://www.caveonix.com/platform/riskforesight> |
| **How can someone ensure their resources are configured securely?** |
| IBM Cloud Security and Compliance Center provides on-going insights into the configuration of the resources for virtual private cloud services.  Client security or compliance Focals can use this information to ensure that the organization is adhering to the external and internal standards for their industry. They can also identify potential issues as they arise. With Security and Compliance Center, Administrators can monitor for controls that pertain to the VMware Solutions infrastructure and workloads.  In non-VMware environments, with IBM Cloud® Security and Compliance Center, clients can embed security checks into routine workflows to help monitor risks. By using the Configuration Governance component of the service, clients can create and manage configuration rules and resource templates for IBM Cloud® resources.  Rules and templates provide a granular approach for governing how resources across client IBM Cloud accounts can be provisioned and configured. With rules, clients can enforce conditions and actions to set guardrails around specific IBM Cloud resource types. And, with templates, clients can define their preferred default values for resources in their accounts. To start enforcing a rule or using a template, clients attach it to one or more organizational scopes, such as account groups, individual accounts, or an entire enterprise.  For additional information:   * Caveonix RiskForesight™: <https://cloud.ibm.com/docs/vmwaresolutions?topic=vmwaresolutions-caveonix_considerations> * Caveonix – Creating a Connection: <https://cloud.ibm.com/docs/security-advisor?topic=security-advisor-setup-caveonix#connect-caveonix> * Caveonix Schedule Security Advisor Job: <https://cloud.ibm.com/docs/security-advisor?topic=security-advisor-setup-caveonix#caveonix-job> * Security and Compliance Center (SCC): <https://cloud.ibm.com/docs/security-compliance?topic=security-compliance-getting-started> |
| **How does IBM propose to implement a shared responsibility model reporting on compliance of IBM controls and enabling a client bank control reporting for its owned controls?** |
| The control requirements from NIST 800-53 used within the IBM Cloud Framework for Financial Services is sufficiently abstract for financial services organizations to have their own interpretation of how they will implement the controls based on the risk tolerance of their organization and the regulators providing guidance. There is no universal security solution. The risk tolerance and interpretation of risk is defined by the clients in the solution implementation.  As organizations move to cloud, roles and responsibilities change with the Cloud Service Provider (CSP) taking on more responsibilities to deliver platform capabilities - including security and compliance. The demarcation between the areas of responsibility in the Shared Responsibility Model is known as the Line of Shared Responsibility (LoSR) as illustrated below. Allocation of services in the Shared Responsibility Model may vary depending on the CSP and cloud service models.  Cloud service users, such as financial services organizations, are responsible for functions / activities above the LoSR (above-the-line). Governance and service levels for the hybrid cloud computing environment define and manage the hand-offs, overlaps and gaps between systems, service providers, locations, etc. The requirement to perform many of the operational tasks, such as maintenance, enhancements and monitoring, passes to the CSP. This includes a reliance on the CSP to ensure the security of the infrastructure, remediate vulnerabilities and respond to incidents in a timely manner.  As the responsibilities move, the level of control and transparency is reduced. Much of the ability to approve changes that might impact the availability of the service are now gone. High-priority security maintenance of the infrastructure could happen in days or hours requiring interruption to individual services in an availability zone. Applications need to be built to be resilient to individual availability zone maintenance outages.  Transparency of the security below-the-line may not be visible including vulnerabilities with the risk mitigation down to the CSP. The implementation of the infrastructure is not exposed and there needs to be trust in the CSP to remediate vulnerabilities rapidly. The Security and Compliance Center (SCC) provided as a part of IBM Cloud is a key service to improve the visibility of these controls.  Banks will have access to relevant reporting data from IBM Cloud for Financial Services in VMware and non-VMware environments.  **Compliance Reporting**  IBM Cloud compliance results from a platform and services that are built on best-in-industry security standards, including GDPR, HIPAA, ISO 9001, ISO 27001, ISO 27017, ISO 27018, PCI, SOC2, and others.  **Compliance Reports**  IBM Cloud provides compliance reports for some compliance regulations, for example SOC or PCI, to advise clients. The reports include details of the audit experience and can help users assess and address the high, medium, and low risks identified.  All requests must go through the formal process. Do not direct to individuals as they will be sent right back to route the request through formal process.  For additional information:   * Compliance on the IBM Cloud: <https://www.ibm.com/cloud/compliance> * If you have an IBM Cloud account and want an infrastructure compliance report, go to: <https://cloud.ibm.com/classic/security/compliancereport/request>. Fill out the form to receive an email with the requested reports attached. * If you don't have an IBM Cloud account or want a PaaS compliance report, go to <https://www.ibm.com/account/reg/us-en/signup?formid=MAIL-wcp>. Fill out the form and you will be contacted by an IBM representative. |
| **Will IBM still comply with existing industry standards?** |
| Yes. IBM adopts and aligns with all relevant and applicable industry standards.  The Framework for Financial Services will not replace our need to comply with industry standards such as SOC, ISO, PCI, etc. Our cloud service’s compliance to the framework does not replace our intention to maintain compliance with existing global and regional standards or compliance programs. Our commitment to these standards remains in place.  Standard global compliance programs e.g., ISO, SOC, PCI, will continue to be conducted with compliance achieved or certified at the IBM's public cloud service level.  As such, individual FS Cloud validated services will continue to maintain their individual compliance posture.  An internal view of the compliance posture per cloud service can be found on the IBM public cloud Compliance Dashboard.  For additional information:   * IBM compliance website: <https://www.ibm.com/cloud/compliance> * IBM Compliance Dashboard: <https://www.ibm.com/w3-techblog/compliance/> |
| **How are controls related to managed services and APIs integrated into the client bank preventative and detective control operating effectiveness reporting?** |
| Clients will have the option of either directly viewing or importing relevant logs into an existing system for additional applications and environments.  The controls will be the same but the approach to delivering the control will be different. Consider these as commonalities in the “what” but differences in the “how.”. |
| **Are regulators endorsing the IBM Cloud for Financial Services™?** |
| No. Regulators do not endorse products, platforms, or services as it introduces bias and conflicts of interest. But IBM and Promontory regularly engage with regulators and are, if appropriate, sometimes asked to review and contribute recommendations to new or updated regulations. Example: IBM participated in the European Banking Authority recent drafting of the EBA revised Guidelines on outsourcing arrangements. |
| **Can IBM provide an audit report on our operating environment (SOC2 type)?** |
| Yes. Please see the links below for more details on the compliance posture of and how to request compliance evidence and artifacts for the underlying FS Cloud services including cloud native and VMware.  For additional information:   * External IBM Cloud compliance programs page: <https://www.ibm.com/cloud/compliance> * Internal: <https://www.ibm.com/w3-techblog/compliance> * IBM Privacy Shield: <https://www.ibm.com/privacy/privacy-shield> * Privacy Shield Program and to view the certification applicable to certain IBM Cloud Services:  [www.privacyshield.gov](https://www.privacyshield.gov/welcome) |
| **Does IBM FS Cloud support least privilege policies for applications accessing cloud resources?** |
| Yes. IBM Cloud infrastructure and IBM Cloud platform restrict access to administrative tools and utilities via an IBM Cloud platform User Access Management tool and access is based on least privilege and best practices. Approval is required from both the employee manager and the system access owner. All successful and failed logins and all privileged actions are logged.  For additional information:   * Working with resources and resource groups (ibmcloud resource); <https://cloud.ibm.com/docs/cli?topic=cli-ibmcloud_commands_resource>[https://cloud.ibm.com/docs/security-compliance?topic=security-compliance-getting-started](file:////Users/brettsibmmacair/Documents/00%20-%20Cloud%20Engagement%20Hub/00%20-%20Sales%20Support/00%20-%20FAQ%20and%20Field%20Guide%20for%20IBM%20Cloud%20for%20Financial%20Services/00%20-%202021-1Q%20FS%20Field%20Guide/Draft%20versions/•https:/cloud.ibm.com/docs/security-compliance%3ftopic=security-compliance-getting-started) * External VMware reference: <https://docs.vmware.com/en/VMware-Validated-Design/services/introduction-to-security-and-compliance/GUID-4AC44907-43DA-4CD5-AA6C-46221D7589F2.html> |
| **Does IBM FS Cloud support identification of anomalous user activity and have ability to send alerts to client's SIEM?** |
| IBM Cloud provides connectivity “hooks” into our IAM services and sends event logs to a client’s own SIEM system. Discussions with the client are required to understand the risk profile and existing Identify Access Management solutions that exist in their environment to determine the optimal approach. Depending on what the client is using for software, that may be integrated into the solution environment.  For additional information:   * IBM Cloud Identity and Access Management; <https://cloud.ibm.com/docs/account?topic=account-iamoverview> * Log Analysis with LogDNA; <https://cloud.ibm.com/docs/Log-Analysis-with-LogDNA> |
| **Does IBM FS Cloud support logs only being accessible to users with a legitimate business requirement and protecting logs from unauthorized modification or deletion?** |
| IBM 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 IBM 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, providing:   * 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. * IBM Cloud Security and Compliance Center: this platform and dashboard provides a unified experience to view and manage security and compliance postures. Security engineers and application developers are able to quickly identify security risks and vulnerabilities, as well as govern cloud resource configurations and centrally manage their compliance to their organization and regulatory guidelines.   The IBM Cloud is the most secure cloud offered. IBM offers Hyper Protect Crypto Services as a single-tenant Key Management Service and a Cloud Hardware Security Module (HSM) service. Key vaulting is provided by dedicated, client-controlled cloud HSMs that are built on FIPS 140-2 Level 4-certified (tamper-proof) hardware, the highest offered by any cloud provider in the industry. The service offers Keep Your Own Key (KYOK) capabilities, which allow clients to have exclusive key control— only authorized users have access (no privileged users, including IBM Cloud Administrators, have access) to encryption keys.  As reference, Federal Information Processing Standard Publication 140-2 (FIPS PUB 140-2) is the National Institute of Standards and Technology (NIST) defines the requirements and standards for cryptography modules that include both hardware and software components. Protection of a cryptographic module within a security system is necessary to maintain the confidentiality and integrity of the information protected by the module. This standard specifies the security requirements that will be satisfied by a cryptographic module. There are four increasing qualitative levels of security, including:   * cryptographic module specification * cryptographic module ports and interfaces * roles, services, and authentication * finite state model; physical security * operational environment * cryptographic key management * electromagnetic interference / electromagnetic compatibility (EMI/EMC) self-tests; design assurance * mitigation of other attacks   Federal agencies and departments validate that the module in use is covered by an existing FIPS 140-1 or FIPS 140-2 certificate that specifies the exact module name, hardware, software, firmware, and/or applet version numbers. A commercial cryptographic module is also commonly referred to as a hardware security module (HSM).  Level 1: Security Level 1 provides the lowest level of security. Basic security requirements are specified for a cryptographic module (e.g., at least one Approved algorithm or Approved security function shall be used). No specific physical security mechanisms are required.  Level 2: Security Level 2 requires features that show evidence of tampering, including tamper-evident coatings or seals that must be broken to attain physical access to the plaintext cryptographic keys and critical security parameters (CSPs) within the module, or pick-resistant locks on covers or doors to protect against unauthorized physical access.  Level 3: Security Level 3 attempts to prevent the intruder from gaining access to CSPs held within the cryptographic module. Physical security mechanisms required at Security Level 3 are intended to have a high probability of detecting and responding to attempts at physical access, use or modification of the cryptographic module. The physical security mechanisms may include the use of strong enclosures and tamper-detection/response circuitry that zeroes all plaintext CSPs when the removable covers/doors of the cryptographic module are opened.  Level 4: Security Level 4 is the highest level of security. The physical security mechanisms provide a complete envelope of protection around the cryptographic module with the intent of detecting and responding to all unauthorized attempts at physical access. Penetration of the cryptographic module enclosure from any direction has a very high probability of being detected, resulting in the immediate deletion of all plaintext CSPs.  Security Level 4 also protects a cryptographic module against a security compromise due to environmental conditions or fluctuations outside of the module's normal operating ranges for voltage and temperature. A cryptographic module is required to either include special environmental protection features designed to detect fluctuations and delete CSPs, or to undergo rigorous environmental failure testing to provide a reasonable assurance that the module will not be affected by fluctuations outside of the normal operating range in a manner that can compromise the security of the module. Security Level 4 cryptographic modules are useful for operation in physically unprotected environments.  For additional information:   * Protecting sensitive information in your cluster: <https://cloud.ibm.com/docs/containers?topic=containers-encryption> * NIST 140-2 Security Requirements for Cryptographic Modules: <https://csrc.nist.gov/publications/detail/fips/140/2/final> * Getting started with Security and Compliance Center: <https://cloud.ibm.com/docs/security-compliance?topic=security-compliance-getting-started> * Key Protect Architecture and Workload Isolation: <https://cloud.ibm.com/docs/key-protect?topic=key-protect-compute-isolation> |
| **What separation is suggested for different SDLC environments, such as Dev, SI, Prod? How is this separation achieved?** |
| Multiple deployment environments are common when building a solution. They reflect the lifecycle of a project from development to production. Tools such as IBM Cloud Command Line Interface (CLI) and Terraform may be used to automate the creation and maintenance of these deployment environments.  Using separate environment clusters is recommend, using DevOps automation with Tekton pipelines to deploy to each environment. A good practice may use separate Schematics workspaces for each deployment environment. Tekton is a flexible open-source framework for creating continuous integration and either continuous delivery or continuous deployment (CI / CD) systems allowing developers to work in separate development, test, and production environments effectively and efficiently.  There are multiple methods including but not limited to physical and logical separation additionally IBM can provide guidance for operating model modernization to ensure that relevant security best practices and DevSecOps. Developers do not like to write the same thing twice. The Don’t Repeat Yourself (DRY) principle is one example of this. Similarly, they don't like having to go through tons of clicks in a user interface to setup an environment. Consequently, shell scripts have been long used by system Administrators and developers to automate repetitive, error-prone and uninteresting tasks.  Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Container as a Service (CaaS), Functions as a Service (FaaS) have given developers a high level of abstraction and it became easier to acquire resources like bare metal servers, managed databases, virtual machines, Red Hat OpenShift clusters, etc. But once a client has provisioned these resources, they need to connect them together, to configure user access, to update the configuration over time, etc. Being able to automate all these steps and to repeat the installation, configuration under different environments is a must-have these days.  Some best practices for organizing users, teams, applications may include:  Graphical user interface, text, application, email  Description automatically generated  For additional information:   * Teraform: <https://www.terraform.io/> * Tekton: <https://tekton.dev/> * IBM Cloud CLI: <https://www.ibm.com/cloud/cli?lnk=STW_US_STESCH&lnk2=learn_CloudDevCLI&pexp=DEF&psrc=NONE&mhsrc=ibmsearch_a&mhq=IBM%20Cloud%20CLI> * Best practices for organizing users, teams, applications: <https://cloud.ibm.com/docs/solution-tutorials?topic=solution-tutorials-users-teams-applications#users-teams-applications> * Plan, create and update deployment environments: <https://cloud.ibm.com/docs/solution-tutorials?topic=solution-tutorials-plan-create-update-deployments> |
| **How does IBM Cloud for Financial Services integrate with client's Global Authorization solution for authentication and multi-factor authentication (MFA)?** |
| IBM Cloud supports integration with third party tools authentication and Multi-Factor Authentication (MFA).  IBMid supports federation with any Identity Provider (IDP) that uses Security Assertion Markup Language (SAML) 2.0. This will create an IBMid for each federated user as they log in. Those federated users can be added to cloud accounts and assigned access, either statically or via dynamic access group membership based on SAML rules. If MFA is done in the IDP, it must be enforced in the IDP - if the IDP logs a user in and returns them to IBMid, it is assumed that if MFA was required for this user the IDP prompted them and would not log them in if MFA were not supplied. There is an IBM Cloud account setting that allows you to indicate that MFA is not required, required only for non-federated users, or required for all users. If MFA is enforced in your IDP, you should set this to either not required or required only for non-federated users, otherwise users will be prompted twice for MFA - once by the IDP and a second time by IBMid. |
| **Does IBM Cloud for Financial Services support data encryption keys being rotated on at least an annual basis?** |
| Yes. IBM Cloud for Financial Services supports alternatives for data encryption key rotation including:   * Setting a rotation policy: the simplest key rotation option, setting an automatic rotation interval means root keys are updated without further effort from the user. These rotations can be set at 30-day intervals (in other words, every 30 days, or 60 days, or 90 days, up to 12 months, or 720 days). This policy can be managed in the UI or by using the Key Protect API. For more information about how to set a rotation policy, check out Setting a rotation policy. The process can also be set using the CLI. * Rotating keys manually: a Security Administrator might want to have more control over the frequency of rotation for their root keys. If they don't want to set an automatic rotation policy for a key, they can manually create a new key to replace an existing key, and then update their applications so that they reference the new key.   To simplify this process, they can use Key Protect to rotate the root key at any time. In this scenario, Key Protect creates and replaces the key on their behalf with each rotation request. The metadata and key ID of the key will not change.  It is a best practice to rotate root keys (that is, to create a new version of the key) on a regular basis. Regular rotations reduce what is known as the "cryptoperiod" of the key and can also be used in specific cases such as personnel turnover, process malfunctions, or the detection of a security issue. If you suspect a key has been compromised, disable it as soon as possible.  Root keys are used to create data encryption keys (DEKs) but are also used in conjunction with a master key (secured by IBM using a Hardware Security Module) to create a "wrap" of a data encryption key (DEK). The resulting "wrapped data encryption key" (WDEK) protects the DEK, which is used to encrypt data. If a user has a DEK they want to use, that key can be passed when creating a WDEK using the wrap call. If no DEK is specified, Key Protect creates the DEK for the user.  Rotating to a new version of the root key does not immediately create a new WDEK, but it does mean that on the next wrap and re-wrap initiated by the user that the new root key will be used to create the new WDEK. Note that the new WDEK can also be unwrapped and used to read data encrypted with older versions of the DEK, and that old versions of the WDEK can still be unwrapped to obtain the DEK.  For additional information:   * Rotating root keys: <https://cloud.ibm.com/docs/key-protect?topic=key-protect-key-rotation> * Key Protect: <https://cloud.ibm.com/catalog/services/key-protect#about> * Manually rotating keys: <https://cloud.ibm.com/docs/key-protect?topic=key-protect-rotate-keys> |
| **Does IBM Cloud for Financial Services support client data processed or stored in the cloud environment must be monitored and subject to Data Loss Prevention (DLP) scans with applicable controls?** |
| Yes. IBM uses five key practices in our Critical Data Protection Program, including:   * Discover: assesses current data environment and completes the data discovery process through data analysis * Classify: organizes data by relevant categories so that it may be used and protected more efficiently * Establish data security strategy: assesses and scores current data security processes by performing gap analysis and developing risk mitigation roadmap * Protect: plans, designs and implements critical data security solutions including data loss prevention, encryption and cryptographic services * Monitor: determines governance process and metrics to enable monitoring, communications and response for data security   For additional information:   * IBM Critical Data Protection Program: <https://www.ibm.com/security/services/critical-data-protection-program> |
| **Does IBM Cloud for Financial Services support stateful packet inspection be required for inbound -outbound network internet traffic for public IaaS & PaaS environments and packet inspection for private cloud done at core network perimeter?** |
| Yes. IBM Cloud® offers several firewalls (dedicated or shared) to choose from and the following support stateful pack inspection:   * Fortinet Fortigate virtual appliances are an option in the VMWare solution portfolio. They can be used to provide a number of next generation firewalling capabilities like IDS/IPS, Layer 7 control, etc. at the Internet edge of the client’s VMWare environment. * Juniper SRX Firewall is another firewall appliance in the VMWare solution portfolio. These firewalls provide the same capabilities as the Fortinet firewalls with slight variances.   As reference:  Fortigate is not specific to VMware runtime  Fortigate has historically been an option that people can deploy as firewalls and ips/ids   * Fortigate has been used as firewalls in “classic” environments   IBM’s hardware firewall leverages a multi-tenant enterprise platform to protect an individual server. It can be purchased with the server or added on later. It delivers virtualized network security through its Virtual Domain (VDOM) technology, providing virtualized security domains that are separately provisioned and managed. Up to 79 firewall rules can be configured for the primary and statically routed IP addresses assigned to the server. Reports for firewalls are available based on the activity of a single IP for a selected date range. Clients can manage the firewall in two ways: through the IBM Cloud console (the firewall tab under the protected server details page) or through SLDN APIs.  Virtual and Physical security appliances can be deployed in the environment with next generation firewall capabilities at the client’s discretion with client determined polices for packet inspection or any other type of Intrusion Detection Systems (IDS) or Intrusion Prevention Systems (IPS).  The client can control the flow of network traffic in their VPC by configuring VPC routes. Use VPC routes to specify the next hop for packets, based on their destination addresses.  For additional information:   * FortiGate Virtual Appliance overview: <https://cloud.ibm.com/docs/vmwaresolutions?topic=vmwaresolutions-fortinetvm_considerations> ) * Routing tables and routes: <https://cloud.ibm.com/docs/vpc?topic=vpc-advanced-routing> * IBM Cloud Security Architecture: <https://www.ibm.com/cloud/architecture/architectures/securityArchitecture/security-for-network/> * IBM Cloud Firewall Options: <https://cloud.ibm.com/docs/security-groups?topic=fortigate-10g-exploring-firewalls&mhsrc=ibmsearch_s&mhq=stateful%20packet%20inspection> * Fortigate: <https://www.fortinet.com/products/next-generation-firewall> * Juniper Networks: <https://www.juniper.net/us/en/solutions/security/next-gen-firewall/> * Migrating FortiGate Security Appliance 1Gbps: <https://cloud.ibm.com/docs/fortigate-1g?topic=fortigate-1g-migration-overview> * Migrating Hardware Firewall (Dedicated): <https://cloud.ibm.com/docs/hardware-firewall-dedicated?topic=hardware-firewall-dedicated-migration-overview#migration-overview> * Specific to Classic, in VPC there are:   + Checkpoint: <https://cloud.ibm.com/catalog/content/checkpoint-iaas-gw-ibm-vpc-1.0.7-9ed8dbde-2931-45f5-a7a7-0c90ce0d2686-global#about>   + Palo Alto: <https://cloud.ibm.com/catalog/content/ibmcloud-vmseries-1.9-6470816d-562d-4627-86a5-fe3ad4e94b30-global#about>   + F5: <https://cloud.ibm.com/catalog/content/ibmcloud_schematics_bigip_multinic_declared-1.0-d33f1544-e938-478a-b0dd-d883370f08d0-global#about> |
| **Can IBM Cloud for Financial Services resources be configured to prevent direct internet connections unless required for a defined business purpose?** |
| Virtual and physical security appliances can be deployed in the environment with next generation firewall capabilities at the client’s discretion.  The IBM Cloud network integrates three distinct and redundant network architectures into a network-within-a-network topology. Every server is physically connected to public, private, and out-of-band management networks, as shown in the image below.  In this internal, IBM Cloud-specific, triple-network architecture, interfaces are dedicated to different usage purposes, providing for varying levels of security.   * Public network handles public traffic to hosted websites or online resources. Clients can choose to order servers with no public network connectivity, meaning that they are provisioned without a public IP address and are not internet routable. * Private network provides free, secure connectivity between servers housed in any IBM Cloud facility. Bandwidth between servers on the private network is unmetered and free, so that the client can move data from one server to another in any IBM Cloud data center quickly and easily over the private network. * Management network allows for true out-of-band management through a distinct, stand-alone third network. This allows both IBM Cloud automation and client management to be separated from the inter-server traffic on the private network cables.   Clients may also choose their own protected space in the IBM Cloud® with the IBM Cloud Virtual Server for VPC providing the security of a private cloud with the agility of a public cloud.  Security features are integrated into this product at the instance level, at the storage level and at the subnet level. Reduce the total cost of ownership and scale for business growth.  This solution of virtual servers for VPC (virtual private cloud) consist of virtual machines (VMs) within IBM’s VPC infrastructure, a public cloud construct. Virtual servers for VPC enable the deployment of a secured private space in a publicly accessible environment by way of a single-tenant infrastructure in a multitenant public cloud. VPCs are logically isolated networks where cloud compute, storage and networking resources are deployed and used to host business workloads, applications and websites. Like networks in traditional on-premises data centers, VPCs utilize cloud security functions and models that match the functionality of those found in offline data centers.  For additional information:   * Networking Services on IBM Cloud: <https://www.ibm.com/cloud/network> * IBM Cloud Virtual Server for VPC: <https://www.ibm.com/cloud/vpc> * Deploy IBM Cloud Virtual Servers for VPC: <https://www.ibm.com/cloud/smartpapers/virtual-private-cloud/> * The Fundamentals of Networking: <https://www.ibm.com/cloud/learn/networking-a-complete-guide#toc-computer-n-9C7jokVu> * About IBM Gateway Appliance: <https://cloud.ibm.com/docs/gateway-appliance?topic=gateway-appliance-about> * What is Virtualization: <https://www.ibm.com/cloud/learn/virtualization-a-complete-guide?mhsrc=ibmsearch_a&mhq=Virtual%20and%20physical%20security%20appliances%20can%20be%20deployed%20in%20the%20environment> |
| **Can all IBM Cloud for Financial Services data be encrypted in transit and at rest?** |
| Yes. All IBM Cloud platform data can be encrypted in transit and rest.  For additional information:   * The Next Frontier in Security: Confidential Computing: <https://newsroom.ibm.com/confidential-computing> * IBM Cloud Security: <https://www.ibm.com/cloud/security> * IBM Cloud Object Storage: <https://www.ibm.com/cloud/object-storage/details> |
| **Can a client restrict what cloud services are available to developers in the different environments? How?** |
| IBM Cloud Identity and Access Management (IAM) enables Administrators to securely authenticate users for platform services and control access to resources consistently across IBM Cloud. A set of IBM Cloud services is enabled to use IBM Cloud IAM for access control and are organized into resource groups within the client’s account so they can provide users access quickly to more than one resource at a time. Each of these services is labeled as "IAM-enabled" in the catalog. Administrators can use IAM access policies to assign users and service IDs access to resources within the account and group users and service IDs into an access group to easily give all members of the group the same level of access.  Two fundamental concepts in IAM are identity management and access management. These concepts are defined below.  Identify Management:   * The identity concept consists of user identities, service and app identities, API keys, and resources. Users are identified by their IBMid, SoftLayer, or AppID user ID. Service IDs are a second type of identity that is used in an account. Service IDs are used to provide a separate identity for services and applications. Clients can create a service ID to be used by an application that needs access to their IBM Cloud services so that individual user credentials don't need to be used. IBM Cloud API keys are used to authenticate with an API or CLI as a user or service ID. These API keys are provided through IBM Cloud IAM and can't be used generally to authenticate with IBMid outside of IBM Cloud. Clients can also use a single classic infrastructure API key to access classic infrastructure APIs; however, this is not required as they can use IBM Cloud API keys to access the same APIs. * The final piece of the identity concept in IAM is IBM Cloud resources, which are identified by their cloud resource names (CRN).   Access Management:   * The concept of access management consists of a few interrelated components, including users, service IDs, access groups, resources, policies, roles, actions, and the IBM Cloud IAM control system, which allows users to take actions on resources within an account. * IBM Cloud IAM follows an eventually consistent pattern that is common to many cloud-native services. As a result, IAM remains highly available and performant across multiple global regions. Changes that are made to IAM access policies, authorizations, service IDs, API keys, access groups, resource groups, users, or any other access controls are recorded and propagated across all IAM components and IAM-enabled services worldwide. Access changes might not take effect until the propagation process is complete.   The Administrator of the account can also create private catalogs for their accounts. They can define what services can be made available in the product catalogs. Today, the Administrator will have to set this up at the individual account level. IBM does support it using the enterprise model, but it is on our development roadmap.  For additional information:   * Managing Resource Groups: <https://cloud.ibm.com/docs/account?topic=account-rgs> * Setting up Access Groups: <https://cloud.ibm.com/docs/account?topic=account-groups> * Managing Private Catalogs: <https://cloud.ibm.com/docs/account?topic=account-manage-catalog> * Cloud Resource Names: <https://cloud.ibm.com/docs/account?topic=account-crn> |
| **Can a client grant temporary (time-based) access to administrative permissions in higher environments (SI/Prod)?** |
| IBM Cloud does not provide time-based access; however, administrative access is typically granted based on least required privilege, so user access can be managed with automation driven by ticketing systems to give the users the required privileges when the ticket is open, and then remove these privileges when the ticket is closed.  To accomplish this, an Administrator would set up an access group with the desired temporary permissions and create a SAML rule on that access group adding users with a particular SML group membership to the access group. Then, in order to grant a user temporary access, add the user to that group in the IDP, and when their access should be removed, remove them from that IDP group. Setting up dynamic access group rules generally allows Administrators to manage access from their IDP by adding and removing users to groups in the IDP. Once initial setup of the access groups and rules has been done, changing them is unnecessary unless adding a new type of access not already configured for a group is required.  Note: this requires addition additional client effort or development (third party or custom application).  For additional information:   * IAM roles and actions: <https://cloud.ibm.com/docs/account?topic=account-iam-service-roles-actions> * vRealize Cloud Management: <https://www.vmware.com/products/vrealize-cloud-management.html> |
| **Can traffic at public internet boundaries be monitored and with all known malicious IP addresses blocked?** |
| Yes. Virtual and Physical security appliances can be deployed in the environment with next generation firewall capabilities at Delta's discretion.  Administrators can control the flow of network traffic in their VPC by configuring VPC routes. Administrators use VPC routes to specify the next hop for packets, based on their destination addresses.  For additional information:   * VPC Routing and Tables: <https://cloud.ibm.com/docs/vpc?topic=vpc-advanced-routing> * Security architecture for cloud applications: <https://www.ibm.com/cloud/architecture/architectures/securityArchitecture/security-for-network> |
| **Can public IaaS and PaaS environments have an automated Intrusion Detection / Prevention System (IDS/IPS) in place for all inbound and outbound internet traffic?** |
| Virtual and Physical security appliances can be deployed in the environment with next generation firewall capabilities at the client’s discretion  Administrators can control the flow of network traffic in the VPC by configuring VPC routes. Use VPC routes to specify the next hop for packets, based on their destination addresses.  For additional information:   * Routing tables and routes: <https://cloud.ibm.com/docs/vpc?topic=vpc-advanced-routing> * IBM Cloud Hyper Protect Crypto Services: <https://cloud.ibm.com/docs/hs-crypto?topic=hs-crypto-overview> |
|  |
| **Can public endpoints be protected using a combination of a content delivery network (CDN) and a web application firewall?** |
| Yes. The client can control the flow of network traffic in their VPC by configuring VPC routes. Use VPC routes to specify the next hop for packets, based on their destination addresses.  IBM’s hardware firewall leverages a multi-tenant enterprise platform to protect an individual server. It can be purchased with the server or added on later. It delivers virtualized network security through its Virtual Domain (VDOM) technology, providing virtualized security domains that are separately provisioned and managed. Up to 79 firewall rules can be configured for the primary and statically routed IP addresses assigned to the server. Reports for firewalls are available based on the activity of a single IP for a selected date range. Clients can manage the firewall through two ways: the IBM Cloud console (the firewall tab under the protected server details page) and SLDN APIs.  Virtual and Physical security appliances can be deployed in the environment with next generation firewall capabilities at the client’s discretion with client determined polices for packet inspection or any other type of Intrusion Detection Systems (IDS) or Intrusion Prevention Systems (IPS).  Fortigate, Juniper, or other client supplied virtual fire walls may be integrated into IBM Cloud for Financial Services configurations.  For additional information:   * IBM Cloud Security Architecture: <https://www.ibm.com/cloud/architecture/architectures/securityArchitecture/security-for-network/> * IBM Cloud Firewall Options: <https://cloud.ibm.com/docs/security-groups?topic=fortigate-10g-exploring-firewalls&mhsrc=ibmsearch_s&mhq=stateful%20packet%20inspection> * Fortigate: <https://www.fortinet.com/products/next-generation-firewall> * Juniper Networks: <https://www.juniper.net/us/en/solutions/security/next-gen-firewall/> |
|  |
| **Are insecure and unencrypted protocols blocked in all cloud environments?** |
| Virtual and Physical firewall appliances can be deployed in the environment at the client's discretion  IBM Cloud Identity and Access Management (IAM) can be used to grant permissions to IBM Cloud Schematics and the IBM Cloud resources that the client wants to provision. They will need to utilize resource groups in order to ensure that infrastructure as a code will not be able to go beyond its set limitations.  For additional information:   * IBM Cloud Schematics access: <https://cloud.ibm.com/docs/schematics?topic=schematics-access>   Open in public can be restricted by firewall FS is off by default unless open |
| **Is access to IBM’s resources strictly controlled to ensure only those with a required need to access such services are permitted and that only the appropriate level of access is allowed?** |
| Yes. IBM Cloud Identity and Access Management (IAM) enables Administrators to securely authenticate users for platform services and control access to resources consistently across IBM Cloud. A set of IBM Cloud services is enabled to use IBM Cloud IAM for access control and are organized into resource groups within the client’s account so they can give users access quickly to more than one resource at a time. Each of these services is labeled as "IAM-enabled" in the catalog. Administrators can use IAM access policies to assign users and service IDs access to resources within the account and group users and service IDs into an access group to easily give all members of the group the same level of access. Note: For services that don't support the use of IBM Cloud IAM policies for managing access, clients can use Cloud Foundry access or classic infrastructure permissions.  Industry-leading FIPS 140-2 Level 4 encryption for technology assured safeguarding of data via Confidential Computing and Keep Your Own Key.  The IBM Cloud is the most secure cloud offered. IBM offers Hyper Protect Crypto Services as a single-tenant Key Management Service and a Cloud Hardware Security Module (HSM) service. Key vaulting is provided by dedicated, client-controlled cloud HSMs that are built on FIPS 140-2 Level 4-certified (tamper-proof) hardware, the highest offered by any cloud provider in the industry. The service offers Keep Your Own Key (KYOK) capabilities, which allow clients to have exclusive key control— only authorized users have access (no privileged users, including IBM Cloud admins, have access) to encryption keys.  .    Figure: How access management works in an account by using IAM  For additional information:   * IBM Cloud Identity and Access Management: <https://cloud.ibm.com/docs/account?topic=account-iamoverview> * Cloud Foundry Access: <https://cloud.ibm.com/docs/account?topic=account-cfaccess> * Classic Infrastructure Permissions: <https://cloud.ibm.com/docs/account?topic=account-infrapermission> * IBM Cloud compliance programs: <https://www.ibm.com/cloud/compliance> * Getting started with Security and Compliance Center: <https://cloud.ibm.com/docs/security-compliance?topic=security-compliance-getting-started> * VMware Docs - Security Principles: <https://docs.vmware.com/en/VMware-Validated-Design/services/introduction-to-security-and-compliance/GUID-4AC44907-43DA-4CD5-AA6C-46221D7589F2.html> |
| **What cloud audit log information from IaaS and PaaS environments is able to be collected and integrated with the client SIEM tool?** |
| A list of event information is outlined in product documentation. Example events may include:   * User ID * Time * Type of event (log in, log off, resource creation, resource modification, etc.) * System information such as resource name, data, etc. and include:   + Success or failure of event   + Source IP address of call   + Identifier/Name of affected resource(s) |
| **Can both environments exist at the same time (VMware and non-VMware)?** |
| Yes. Please consult IBM Cloud, or IBM Consulting for discussion of appropriate approaches. |
|  |
|  |
|  |
|  |
| **How will a bank need to change its operating model to enable the IBM Cloud for Financial Services™ e.g., organizational maturity level within a cloud adoption framework?** |
| For any use of public cloud, clients’ operating models will be affected in many ways including: hiring staffing, management, development, deployment, and access and usage of data. IBM has successfully helped many clients through this skills and process transformation and offers Garage engagements, Services, Cloud Advisory, IT Services, and Cloud Center of Excellence models to enable a successful journey end-to-end to public cloud. All of these IBM practices apply to our clients looking to use the IBM Cloud for Financial Services™. A transformation program can be expected to start by evolving existing processes within the IT function and expanding change to create a new IT governance structure, culture and IT organization structure. Expect the information to affect at least five (5) areas of decision-making: IT principles, IT architecture, IT infrastructure, business application needs, and IT investment. |
| **When will cloud-native services be available?** |
| Virtual Private Cloud services with IBM Cloud for Financial Services were released 1Q.2021 and are available in the IBM Cloud Catalog with a Financial Services Validated designation. These services include:   * Red Hat OpenShift on IBM Cloud * IBM Virtual Server for Virtual Private Cloud * IBM Cloud Object Storage * IBM Block Storage for Virtual Private Cloud * Virtual Private Cloud services |
| **What is the roadmap for IBM PaaS and SaaS services to be available on IBM Cloud for Financial Services™? For example, when will Watson APIs, managed API services be available?** |
| Initial IBM PaaS services with IBM Cloud for Financial Services, including Red Hat OpenShift on IBM Cloud (ROKS) and IBM Cloud Object Storage, released 1Q.2021. The roadmap will include IBM software and SaaS services as plans are committed for those offerings. |
| **Will IBM Cloud for Financial Services™ support IBM Cloud Satellite for management of OpenShift?** |
| Yes, with Framework for Financial Services controls in 2H.2021. This will enable hybrid workload extension between on-premises and IBM public Cloud deployments. |
| **Are there technology roadmaps for PaaS and SaaS that can be shared with client banks to aid joint development of controls and limit duplication?** |
| Yes. Contact the Offering Manager |
|  |
| **SOLUTIONING** |
|  |
| **How is capacity and automation (autoscaling) configured and reported via control interfaces into a client bank (development, security, and operations)?** |
| Automation / autoscaling supports improved capacity and resiliency. The setup includes enabling the backend orchestration to add the newly created VSIs to the backend server pool for the cloud load balancer.  Diagram  Description automatically generated  **Objectives to be achieved include:**   * Create an Auto scale template and group for the VSI * Enable the backend orchestration to add newly created VSIs to the backend server pool for the cloud load balancer   **Services required are:**   * IBM Cloud Virtual Private Cloud * IBM Cloud Virtual Server for Virtual Private Cloud * IBM Cloud Load Balancers * Auto scale   If the client doesn’t have an environment or needs to rebuild their environment, they can use the “Deploying server pools and origins in a single MZR” solution tutorial (link below) to set it up.  For additional information:   * Tutorial for configuring Auto scale ([Enabling Auto scale for better capacity and resiliency](https://cloud.ibm.com/docs/cloud-infrastructure?topic=cloud-infrastructure-ha-auto-scale)): <https://cloud.ibm.com/docs/cloud-infrastructure?topic=cloud-infrastructure-ha-auto-scale> * Deploying server pools and origins in a single MZR: <https://cloud.ibm.com/docs/cloud-infrastructure?topic=cloud-infrastructure-ha-pools-origins> * Enabling autoscale for better capacity and resiliency: <https://cloud.ibm.com/docs/cloud-infrastructure?topic=cloud-infrastructure-ha-auto-scale> |
| **What level of management of the infrastructure is provided? Are OS, patching, and high availability (HA) managed across multiple data centers? Is the scaling managed / automated?** |
| Yes. IBM Cloud provides version information and update actions noted for supported OpenShift versions for Red Hat® OpenShift® on IBM Cloud™ clusters.  Red Hat OpenShift on IBM Cloud clusters have three types of updates: major, minor, and patch. As updates become available, clients are notified when viewing information about the cluster master or worker nodes.  Graphical user interface, text, application, email  Description automatically generated  IBM Cloud also provides for high availability and disaster recovery. The IBM Cloud console is available globally and load balanced from a single URL. It is highly available and continues to run even if resources are unavailable.  Other platform services, including catalogs, global search and tagging, identity and access management, and account management are also globally available and load balanced across multiple regions. A failover design is in place to keep clients’ resources up and running without them having to take action.  Each platform service is categorized as a general availability service with a Service Level Agreement of 99.99% availability. While each platform service might be available from various regions, each region in which the service is deployed has multiple data centers for redundancy.   | **Platform service** | **Details** | | --- | --- | | Account management | [Best practices for setting up your account](https://cloud.ibm.com/docs/account?topic=account-account_setup) and [Best practices for billing and usage](https://cloud.ibm.com/docs/billing-usage?topic=billing-usage-best-practices) | | Catalogs | [Managing catalog settings](https://cloud.ibm.com/docs/account?topic=account-filter-account) | | Table 1. Platform services | | |
| **What is the shared application identity model used across application services?** |
| IBM Cloud uses SAML federation, and several options exist, including:   * **Normal IBMid users:** Users with a valid email address can create an IBMid and let the password be managed by IBMid. * **Federated IBMid users:** Enterprise clients often connect their internal User Directory ("Identity Provider") with IBMid so that their employees do not need to manage an additional password. Instead, they can reuse their normal login to their Identity Provider to also log in to IBMid. Connecting an external Identity Provider with IBMid is called federation, the technical underlying protocol is called SAML, and those users are often referenced as federated IBMid users. As IBMid is federating with multiple enterprise clients at the same time, one prerequisite of a successful federation is a unique email address for each IBMid user. * **IBM Cloud App ID users:** Instances of the IBM Cloud service App ID can also connect to an Identity Provider. An App ID instance can only connect to one external Identity Provider using SAML, therefore there is no requirement for a unique email address.   For additional information:   * IBM Cloud SAML Federation Guide:<https://www.ibm.com/cloud/blog/ibm-cloud-saml-federation-guide> |
| **How does the IBM Cloud for Financial Services control the geographic deployment location the scheduler runs in?** |
| IBM Cloud Identity and Access Management (IAM) enables clients to control which users see, create, use, and manage resources in their account. To grant access, client Administrators can assign roles that allow users levels of access for completing platform management tasks and accessing account resources.  The way that clients manage access in IBM Cloud® depends on the type of resource to whom they want to assign access. IBM Cloud Identity and Access Management (IAM) is the access management system that is used for consistently managing resources that are organized in a resource group across the IBM Cloud platform. Classic infrastructure and Cloud Foundry resources are not managed by using Cloud IAM. These resource types have their own access management systems.  If a client has a combination of resource types, they manage each type separately:   * For IAM resources, Administrators go to Manage > Access (IAM) in the console, and then select Users, Access groups, or Service IDs to get started. * For assigning access to the classic infrastructure resources, the client set permissions within Manage > Access (IAM) on the Classic infrastructure tab for the user that they want to assign access. * For assigning access to Cloud Foundry resources, Administrators assign users to orgs and set Cloud Foundry org and space access roles within Manage > Access (IAM) on the Cloud Foundry tab for the user.   While each type of access is managed separately, all access policies are made up of a subject, clients want to assign access to, a target for the policy to scope what the subject has access to, and then finally an IAM role, Cloud Foundry role, or classic infrastructure permission to determine the level of access the subject has on the target.  For additional information:   * Access management in IBM Cloud: <https://cloud.ibm.com/docs/account?topic=account-access-getstarted> |
|  |
| **What is required to develop, deploy, and maintain applications consistently across any infrastructure?** |
| In order to consistently develop and deploy applications across any infrastructure, organizations must enable portability via container and cloud native features across all their technology environments (including on-premises, AWS, Azure, Google Cloud Platform (GCP), and IBM public cloud infrastructures).  OpenShift provides three (3) advantages for effective containerization and consistent development:   * True Platform as a Service that provides developers and operators with thousands of pre-certified solutions developed by Red Hat and partners, further extended by our Cloud Pak capabilities and partner ecosystem * Heritage middleware and data & AI integration that enables a consistent development lifecycle integrating the IBM workloads that enterprises have relied on to run their mission critical systems * Hundreds of fixes for defect and performance issues that come before each Kubernetes release |
| **What is required to consistently ensure security across hybrid, multicloud environments?** |
| Today, security teams are overwhelmed, managing hundreds of thousands of events each day across disparate systems and the cloud.   * Security and compliance tools must be deeply integrated across all components * The IBM platform provides prioritized threat detection, intelligence, and federated security monitoring across the entire ecosystem of data * IBM Cloud® Security and Compliance Center embeds security checks into everyday workflows to help monitor for security and compliance. * Security and Compliance Center will monitor security and compliance posture in:   + IBM Cloud   + Amazon Web Services   + Google Cloud Platform   + Microsoft Azure   + On-premises   For additional information:   * Security & Compliance Center FAQ: <https://cloud.ibm.com/docs/security-compliance?topic=security-compliance-faqs> |
| **How is control compliance CI/CD [continuous integration (CI) and continuous delivery (CD)] reported in IBM Cloud for Financial Services?** |
| IBM Cloud Framework for Financial Services provides industry-informed controls, implementation and evidence guidance to enable risk management and security protection via common criteria for the ecosystem. Real-time monitoring and continuous compliances are enabled using IBM Cloud tools and solutions. Financial Services partners get on-premises like transparency in the Cloud.  IBM Cloud Security and Compliance Center: <https://cloud.ibm.com/docs/security-compliance> |
| **Does IBM outsource any part of its cloud operations?** |
| No. IBM does not currently outsource any part of our cloud operations to non-IBM entities. |
| **What type of skills do I need to build to operate IBM Cloud for Financial Services?** |
| Common roles to operate IBM Cloud for Financial Services are similar to roles to operate in other clouds. There are nuanced skills related to certain applications used but many of the roles are the same, including:   |  |  | | --- | --- | | * Cloud Architect | * Full-Stack Engineer | | * Security Engineer | * QA Engineer | | * DevOps Engineer | * Network Architect | | * Data Engineer | * Digital Skills Officer | |
|  |
| **MARKETING** |
|  |
| **How does the IBM Cloud for Financial Services™ help banks and financial institutions accelerate compliance efforts while reducing costs and risk to maintain regulatory compliance?** |
| Banks and financial institutions are able to quickly move to migrate applications in the IBM Cloud for Financial Services™ because the controls for hundreds of regulatory requirements are pre-defined. With the VMware solution, configuration is automated, and the environment can be ready to load data in two (2) weeks. The controls addressed have been developed in coordination with large banks. IBM Cloud for Financial Services™ provides clients with accelerated migrations, hundreds of validated technical controls, and hardened security architectures, resulting in accelerated delivery times, reduced costs, and decreased compliance and security risks.  A key point for the IBM Cloud for Financial Services™ is that developing, managing, and maintaining technical controls for complex financial services regulations is expensive and time consuming. The time and costs saved by the bank can be significant. Banks can also feel comfortable that many compliance risks are mitigated with defined controls mapped to specific compliance obligations.  The IBM Cloud Framework for Financial Services establishes the end-to-end operations and management of the controls built into Cloud services and operations and validated with ISV and SaaS provider services. |
| IBM Cloud for Financial Services clients can:   * Accelerate their transformation: focus on app innovation and engineering with access to a rich network of pre-validated partners * Reduce their cost and time to compliance: pre-validated ISVs & SaaS solutions conforming to financial services security and controls * Technical assurance: risk management and compliance automation, continuous monitoring and audit reporting capabilities * On-premises like transparency to cloud, services, 3rd & 4th party risk mitigation to clients, auditors and regulators on demand * Accelerate innovation & unlock new revenue opportunities while reducing cost of compliance   For more information:   * Apply end to end security to a cloud application: <https://cloud.ibm.com/docs/solution-tutorials?topic=solution-tutorials-cloud-e2e-security> |
| **What value does the IBM Cloud for Financial Services™ bring to financial institutions and their ISV channels?** |
| The IBM Cloud for Financial Services™ comprises IBM Cloud services, independent software vendor (ISV), SaaS and financial institution applications that operate in standard IBM Cloud Multi-Zone Regions and which comply with IBM Cloud Framework for Financial Services. The IBM Cloud for Financial Services™ launched in July 2020, beginning with VMware services and now has Virtual Private Cloud services such as Red Hat OpenShift on IBM Cloud available.  In response to the pressure our financial services clients face to innovate, transform, reduce risk and time to market – all while adhering to ever changing security and regulatory requirements – IBM established the IBM Cloud Framework for Financial Services. The Framework provides industry-informed controls, implementation and evidence guidance to enable risk management and security protection via common criteria for the ecosystem. Real-time monitoring and continuous compliances are enabled using IBM Cloud tools and solutions. Financial Services partners get on-premises like transparency in the Cloud.  Demonstration of compliance for digital supply chain partners is significantly faster and cost of complexity of staying current with regulatory changes is reduced. Currently a bank’s average time to onboard an ISV is 12 to 18 months; with IBM Cloud for Financial Services, it’s reduced to weeks. This acceleration in onboarding, means that banks can take advantage of the many products, features, functions, and benefits offered an ecosystem of ISVs and SaaS providers who are validated to a standard controls framework.  In addition to streamlining of ISV onboarding processes, banks can simplify the process of re-certifying their ISVs, which would ordinarily be required periodically, or in the case of new regulations. In addition, IBM Cloud for Financial Services can simplify further regulatory processes like service auditing and cloud service provider (CSP) auditing, which for banks typically consume significant internal resources and/or require external spending. Finally, IBM Cloud for Financial Services can save clients’ money through breach avoidance and remediation.  Beyond the direct and measurable value drivers above, banks can also realize less predictable, “soft dollar” benefits, which have the potential to be even more significant. The reduced likelihood of mega-breaches (which have massive implications for a bank’s reputation) or regulatory penalties can be hard to measure, but obviously significant, given the levels of security and privacy that regulators, and the general public, expect from banks. Banks can also see indirect business benefits from cheaper and faster ISV onboarding, as employees can benefit from using software applications much sooner if a given ISV is part of the IBM Cloud for Financial Services ecosystem. See #86 for a detailed list of value drivers.  ISVs also invest considerable time in demonstrating compliance to banks during onboarding. Their implementation of the Framework significantly reduces that time, effort, and cost - allowing them to acquire more client banks - increasing their revenue volume and velocity. |
| **How can the IBM Cloud for Financial Services™ help banks manage the stream of regulatory requirements and updates for bank workloads or SaaS applications?** |
| IBM Cloud and ecosystem services validated with IBM Cloud for Financial Services comply with the IBM Framework Base Controls (NIST with IBM financial services guidance) that have applicability to worldwide regulatory guidelines. The preconfigured controls and compliance and security posture management via IBM Cloud tools enable financial institutions to reduce time in maintaining their regulatory obligations while using public cloud and their internal audit requirements. The IBM Financial Services Cloud Council and IBM Promontory will inform needed updates to the Framework controls, and participating banks will have access to this expanding capability.  For ongoing regulatory change management, IBM Security Services and Promontory work in the industry and with clients to understand potential and planned regulation changes. Through their advisory consulting services, they educate and prepare our clients to effectively and efficiently address regulatory requirements. The scope of Promontory’s financial regulatory library contains: 24 jurisdictions (23 countries plus EU) and 75 regulatory and standards issuing bodies. |
| **What are the primary value propositions of the IBM Cloud for Financial Services?** |
| Much of the value of IBM Cloud for Financial Services for clients comes from *direct and measurable sources*, especially those pertaining to:  1) ISV/CSP certification and  2) Breach detection + remediation:   * + Initial ISV onboarding/certification (“Day 1”)     - Evidence mapping     - Process Control mapping   + Ongoing ISV re-certification (“Day 2”)     - Event-triggered (new reg)     - Ongoing monitoring     - Service auditing   + CSP certification effort     - Certification     - Service auditing   + Security operations     - Breach detection     - Remediation   Further value comes from less predictable/measurable sources; these should be considered soft dollars for an investment case but have the potential to be even more significant than the direct benefits.   * Reduced likelihood of regulatory penalties * Cost of mega-breaches * Opportunity of rapid SaaS deployment (business benefit) * Improved audit posture (ex. auditor’s confidence in bank) * Reduced reputation risk   In addition, adoption of IBM Cloud for Financial Services is an important part of a client’s hybrid cloud journey – which yields up to 2.5x more value than a public-only strategy. In the context of a client’s overall cloud journey, FS Cloud is a key contributor of technical and financial benefits.  Graphical user interface, application, Word  Description automatically generated  Chart, scatter chart  Description automatically generated  ISV and SaaS providers wanting to join IBM Cloud for Financial Services must attain, maintain and demonstrate adoption of the Framework. IBM experts work closely with ecosystem partners to onboard and validate adherence to the framework resulting in de-risking of ISV/SaaS providers. The common operational criteria and streamlined compliance controls will help banks and ISVs more effectively manage security and compliance.  To summarize, clients can tap into a rich partner ecosystem of ISV/SaaS providers who are fully validated to the Framework; this accelerates innovation and unlocks new revenue opportunities. Onboarding ISVs in weeks (versus 12-18 months) to support emerging technology innovations. Technology-assured, continuous compliance significantly reduces risk, costs of non-compliance, and overhead of 3rd & 4th party risk assessments. Provides on premise like transparency in the Cloud. |
| **What makes IBM the right cloud provider to take on this endeavor?** |
| **A. IBM FS industry expertise**  Amidst a global crisis, the role of financial enterprises has become more vital than ever.  Banks and financial markets are reinventing themselves on the fly while implementing new government programs in weeks instead of years. Meanwhile, security and compliance mandates have not gone away. The industry knows that to stay strong, it must digitize, modernize and help employees adjust to new ways of working. As financial institutions rush to transform how they operate, they value an enterprise partner they can trust, one with industry and regulatory expertise to help clients update applications, automate processes, deliver great client experiences, leverage data, and move to an efficient secure and agile cloud.  IBM has more than 100 years of Financial Services expertise working with regulated, financial workloads and transactions that require the highest levels of security, privacy, regulatory compliance and resilience. We understand these environments like no other vendor.  Add to that our enterprise grade public cloud and the unique Promontory financial regulatory expertise and it is clear why IBM is the trusted partner for this endeavor.  References:   * 92 of the top 100 banks run the core systems on mainframe (<https://www.ibm.com/blogs/systems/ibm-z-the-banking-platform-for-the-future/>) * 90% global credit card transactions are processed on IBM mainframes (<https://www.ibm.com/downloads/cas/VGYAKENA>) * IBM is the largest Enterprise Cybersecurity provider globally with over 8,000 security experts: <https://www.ibm.com/annualreport/assets/downloads/IBM_Annual_Report_2018.pdf>   **B. IBM’s public cloud is designed for mission-critical workloads**   * When it comes to moving sensitive and confidential data to the cloud, especially in regulated industries like financial services, security is of utmost importance. To help meet these demands, IBM’s public cloud has been designed with the exacting demands of the world’s largest and most complex organizations in mind. Read our recent announcements about [IBM’s public cloud data protection and security leadership, open source innovation, and more enterprise grade capabilities](https://newsroom.ibm.com/2019-10-22-Aegean-Airlines-BNP-Paribas-Elaw-Tecnologia-SA-and-Home-Trust-Select-IBM-Cloud-for-Mission-Critical-Workloads) (<https://newsroom.ibm.com/2019-10-22-Aegean-Airlines-BNP-Paribas-Elaw-Tecnologia-SA-and-Home-Trust-Select-IBM-Cloud-for-Mission-Critical-Workloads>) that reinforce IBM Cloud as the best public cloud for mission-critical workloads. * For example, here are two important capabilities that demonstrate our leadership in security and data protection:   + IBM’s public cloud offers the industry’s only commercially available state-of-art cryptographic technology for the cloud called "Keep Your Own Key", giving enterprises the ability to retain control of their own encryption keys -- and the hardware security modules that protect them - so clients are the only ones who can control access to their data. No other cloud offers this.   + IBM’s public cloud security dashboard called IBM Cloud Security and Compliance Center provides centralized security management, is able to detect security misconfigurations so enterprises can better assess their security postures and take corrective actions.   **C.  IBM’s public cloud is the most open and secure public cloud for business**  Open architectures, based on Kubernetes and containers, are driving the next wave of cloud-based business innovation. That’s why IBM has just completed a two-year journey to enhance its public cloud on a foundation of open-source software and enterprise-grade infrastructure. It can deliver solutions and access to innovation backed by deep industry experience.   * **Open innovation and the public cloud optimized for Red Hat OpenShift**   Build and run applications with ease using native cloud services or deploying on managed Red Hat OpenShift—bringing instant deployment, automated vulnerability management, and self-healing resiliency to the industry’s most comprehensive enterprise Kubernetes platform. IBM is a leader of running Kubernetes production workloads at scale with more than 16,000 production clusters deployed, supporting billions of transactions per day. Automated deployment of IBM Cloud Paks provides a seamless out-of-the-box experience.  From the hypervisor to developer tools to advanced services such as blockchain and AI/ML, open source is in our platform DNA.   * **Security leadership with market-leading data protection**   Our 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. The data you store on our cloud is yours and yours alone. We allow you to bring your own key—that no one but you can see—not even us. Build and run your core business applications and workloads with single dashboard visibility and multiplatform portability.   * **Enterprise-grade for reliable and robust workloads**   Only on IBM’s public cloud can you span classic enterprise multi-architecture lift-and-shift and broad VMware migration to cloud native leadership with broad support for Kubernetes, Knative, Istio and Cloud Foundry. We have the #1 public cloud for VMware, and provide cloud migration for Power AIX, IBMi, Z, SAP and all of your mission critical applications. Whether it is bare metal, GPU or dedicated virtual compute, IBM has what you need. IBM’s compute choices and configurable auto-scaling allow clients to help optimize for dynamic, demanding, sensitive and secure workloads   * **Trusted by 47 of the Fortune 50**   For 10 out of 10 of the world’s largest banks, and 8 out of the 10 largest airlines, IBM Cloud stands up to strenuous security, performance and scalability requirements. And with more than 100,000 professionals and consultants redesigning processes, apps, and cloud infrastructures, IBM has the experience needed to help the client craft an effective cloud strategy to realize their business objectives. |
| **What is the business case for IBM Cloud for Financial Services™?** |
| The business case for IBM Cloud for Financial Services™ from Forrester includes:   * 3-Year TCO Savings running VMware on the IBM Cloud for VMware Regulated Workloads versus in-house: 33% * VMware regulated workloads on the IBM Cloud have experienced a CAGR of over 70%. (see below)   + Bring your own license (BYOL) means no duplicate software licenses (VMware, RedHat, SAP)   + Reduced data center costs by avg of 40% over 3 years   + Operations staff can now more efficiently manage VMware workloads, reducing operations efforts by 2/3   + Security efforts around investigation and patching also reduced with IBM Cloud   + Improved application availability, avoiding 4 downtime events per year by Year 3   + Developers are 40% more efficient with access to RedHat OpenShift   + Savings on regulatory and compliance efforts to design, develop, manage, and report on compliance status   Other Key Benefits   * Client confirmed improvements in performance and latency (Forrester) * Client confirmed improved client satisfaction with IBM Cloud investment (Forrester)   Much of the value of IBM Cloud for Financial Services for clients comes from direct and measurable sources, especially those pertaining to:  1) ISV/CSP certification and  2) Breach detection + remediation:   * Initial ISV onboarding/certification (“Day 1”)   + Evidence mapping   + Process Control mapping * Ongoing ISV re-certification (“Day 2”)   + Event-triggered (new reg)   + Ongoing monitoring   + Service auditing * CSP certification effort   + Certification   + Service auditing * Security operations   + Breach detection   + Remediation   Further value comes from less predictable/measurable sources; these should be considered soft dollarsfor an investment case but have the potential to be even more significant than the direct benefits.   * Reduced likelihood of regulatory penalties * Cost of mega-breaches * Opportunity of rapid SaaS deployment (business benefit) * Improved audit posture (ex. auditor’s confidence in bank) * Reduced reputation risk   In addition, adoption of IBM Cloud for Financial Services is an important part of a client’s hybrid cloud journey – which yields up to 2.5x more value than a public-only strategy. In the context of a client’s overall cloud journey, FS Cloud is a key contributor of technical and financial benefits.  Graphical user interface, application, Word  Description automatically generated  A key driver of business value for a client is their level of cloud deployment, which in every industry, but especially the financial services industry, can be hindered by a lack of trust in cloud due to regulatory and security concerns. Given that many FS workloads would not be suitable for a cloud other than IBM Cloud for Financial Services, adoption of FS Cloud is likely to dramatically increase the overall level of cloud deployment. Clients are then able to reap the benefits of cloud that they otherwise would not.  Chart, scatter chart  Description automatically generated  Additional business case materials developed by [Mitch Costom](mailto:Mitch.Costom@ibm.com) (Mitch.Costom@ibm.com), in Cloud Strategy & Business Models to bring to life the operational changes behind the savings and to tell the client how exactly they capture value. These drivers include:   1. Value Drivers 2. Timeline 3. Investment + ROI Analysis   **Value Drivers:** We maintain a “library” of drivers that affect the client’s business; these aren’t model inputs/outputs but qualitative assumptions on the benefits of cloud that roll up to the quantitative assessment. These drivers include:   * Business Acceleration * Revenue Growth * Operating Expenses * Competitiveness * Innovation * ADM Productivity * Developer Productivity * Maintenance productivity * Maintenance cost-avoidance (tech debt) * Infra Cost Efficiency * Unit cost differential * Infra support spend * Utilization Optimization * Maintenance cost-avoidance (tech debt) * Regulatory and Risk * Security risk * Compliance / audit risk * Strategic Optionality * Architecture flexibility * Agility and cost arbitrage   The value derived is found in these categories over these periods:  **Graphical user interface, application  Description automatically generated**  **Timeline:** the time required to achieve run rate benefits depends on the ambition of the journey; there is a limit to how much can be transformed in a year, and clients are likely to go for “quick wins” i.e., easier journeys first.  Graphical user interface, application, Teams  Description automatically generated  **ROI:** we estimate transformation costs for each journey, which can be compared to benefits of the journey; each journey therefore has a different ROI profile, and the client must balance speed, ROI, and absolute savings.  Timeline  Description automatically generated |
| **What costs can client banks avoid by using the controls now provided out of the box?** |
| Clients using the IBM Cloud for Financial Services™ can avoid costs for designing, assessing the security and compliance posture, maintaining compliance, and readying the cloud environment. With the VMware solution, configuring the IBM Cloud for Financial Services™ can be completed within two weeks, including automated deployment of HA and DR.  **Timeline  Description automatically generated**  **Graphical user interface, text, application, email  Description automatically generated**  **Graphical user interface, application  Description automatically generated**  Area:  Risk / Compliance: 9% Revenue   * Risk Management Association: 50% of respondents said they spent between 6% and 10% of their revenue on compliance costs, while another 20% spent less than 5% on compliance. For banks, that has meant less flexibility in designing products (25%) and higher costs for some products (22%); <https://www.bloomberg.com/professional/blog/rising-compliance-costs-hurting-customers-banks-say/> * Federal Reserve Bank of St. Louis: Compliance costs averaged 7% of noninterest expense; <https://www.communitybanking.org/~/media/files/compliance%20costs%20economies%20of%20scale%20and%20compliance%20performance.pdf> * IT Security is 10% of IT Operating Expense (OpEx); <https://www.finextra.com/pressarticle/78229/financial-institutions-spend-an-average-of-10-of-their-tech-budgets-on-cybersecurity> * Cybersecurity cost as a percentage of IT cost. (Includes all capital and operational costs/spending on activities and systems). IBM Institute for Business Value Benchmark. * IT Compliance is 15% of IT Operating Expense (OpEx): <https://securityintelligence.com/news/security-compliance-spend-now-or-pay-later/> |
| **What is the contracting process for IBM Cloud for Financial Services™?** |
| IBM Cloud for Financial Services uses the standard cloud services agreement (CSA). IBM Cloud for Financial Services does not require nor provide additional terms beyond the standard CSA, or terms and conditions within individual service sheets such as with IBM Cloud for VMware Regulated Workloads.    For additional information:   * Services are ordered and provisioned via the IBM Cloud Catalog at [www.cloud.ibm.com](http://www.cloud.ibm.com) |
| **Does charge for ingress and replication within IBM Cloud environments?** |
| No. IBM Cloud does not charge for data ingress and replication in our environments. |
|  |
|  |
| **Are there example playbook / sales cycle approach for solutioning IBM Cloud for Financial Services™ for Banks and ISVs / SaaS?** |
| es, see below as example. The approach may vary based on context, the client’s need for additional support services such as IBM Services, IBM Security Services, Promontory, and other factors.  There are three ways for clients to order Virtual Private Cloud Services:   1. Private API connection to bank-provided console tool 2. Cloud Command Line Interface for banks that require public APIs not be used 3. Cloud Catalog User Interface for banks that accept the use of public API connections, or for non-bank clients    1. Guided ordering via Walkme tour available beginning 2Q.2021 |
| **How do I help client banks engage around the Framework for Financial Services or plan to use IBM Cloud for Financial Services™?** |
| Contact our worldwide GTM and offering teams with context for your client, geo and objective. Whether you are representing an integrated, industry or enterprise account, the GTM team will work with you to determine next steps, which could include:   * A review of the Framework to plan core banking transformation, cloud resiliency or workload migration (e.g., IBM Cloud for VMware Regulated Workloads) with IBM Cloud Engagement Hub * **Note:** IBM does not distribute the Framework controls but rather use a “controls objective” overview and mapping exercise to provide clients with an understanding of the coverage of the controls. * Define a cloud strategy and MVP with IBM Garage for Cloud * Develop governance and regulatory strategies, as well as secure application strategies via IBM Promontory and IBM Security Services |
| **What is the IBM Research Cloud Innovation Lab?** |
| The Cloud Innovation Lab builds on IBM’s leadership in open innovation and is part of our go-to-market engagement with key financial institution clients. It is an opportunity to connect our clients’ developers, data scientists, cloud architects, chief data officers, etc., and business roles with our PhDs and distinguished engineers in IBM Research to learn and build skills with IBM technologies and Cloud architecture through access to next-gen technology experimentation and engagement. The program will include curated projects in the areas of security and compliance, productivity and automation, AI and analytics and intelligent client interaction. |
| **How do reseller partners participate in IBM Cloud for VMware Regulated Workloads?** |
| Since this solution is an expansion of the standard VMware on IBM Cloud offering, resellers with agreements to resell IBM Cloud can use their existing Business Partner account to order this solution the same way they would our standard VMware on IBM Cloud offering. |
| **Are Global System Integrators (GSI) participating in IBM Cloud for VMware Regulated Workloads?** |
| Yes. Various Global Systems Integrators (GSI) are building practices around IBM Cloud for Financial Services™ and have signed partnership agreements. |
|  |
| **What ISV and SaaS providers intend to onboard their offerings to the IBM Cloud for Financial Services™?** |
| Our ISV and SaaS provider partners include horizontal applications (CRM and HR management) and financial-services vertical applications and represent a range of enterprise banking applications (payments, core banking, fraud solutions) to digital-native cloud core-banking applications.  This list of ISV and SaaS providers is growing rapidly; please check for most current listing. Reference URLs and brief descriptions are included in the Appendix.  External logos:    *ISV and SaaS vendor list as of March 17, 2021* |
| With the support of our technology partners, IBM is building innovative solutions that can enhance the offerings of our financial institution clients by transforming everything from the client experience, core banking applications and payments, to risk and compliance management, cybersecurity, financial reporting, and more. Specific examples include developing a digital transformation platform for banking to rapidly bring a user-centric solution to the market; working directly with banks to offer an innovative relationship-based pricing engine as a SaaS offering to accelerate legacy transformation and business agility; and creating a SaaS-based solution to accelerate implementation of risk and compliance management and optimize securities lending and cash management. |
| **Can we consider onboarding the ISVs and SaaS providers that my financial institution client uses or is interested in?** |
| Yes. The ISV onboarding team engages with ISVs and SaaS providers to help recruit and onboard them to the IBM Cloud for Financial Services™. We support the Coverage Teams and ISVs end-to-end by providing solution overviews, coordinating technical workshops, supporting onboarding and the validation process. Contact the ISV onboarding team,. |
| **How can ISVs and SaaS providers participate in the IBM Cloud for Financial Services™?** |
| The ISV onboarding team engages with ISVs and SaaS providers to provide solution overviews, architectural guidance, coordinating technical workshops, supporting onboarding and the validation process with IBM Cloud for Financial Services™. Contact the ISV onboarding team for more information on the onboarding process |
| **What technical assistance is provided to ISVs and SaaS providers?** |
| The ecosystem program for IBM Cloud for Financial Services includes defined processes and documentation to facilitate the onboarding process for ISVs and SaaS providers to IBM Cloud – a System Security Plan template for ISV and SaaS providers, and a Deployment and Configuration Guide for ISV and SaaS providers. This documentation overviews the Framework controls, and provides implementation, evidence and architectural deployment guidance. Optional, fee-based services are available to assist with remediation and readiness activities. When the ISV or SaaS provider is ready to onboard, IBM will validate the provider’s compliance against the Framework. **What is the IBM Financial Services Cloud Council?** The IBM Financial Services Cloud Council(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 IBM Cloud Framework for Financial Services (Framework) by contributing to and prioritizing industry requirements. The Council seeks to materially reduce the risk of cloud consumption across the financial services industry and its SaaS providers by developing a set of standard controls that will be consistently applied across the global banking industry.  The insights gained from the Council inform and influence the Framework. Together, this Council will drive an innovative new construct for public cloud, enabling cloud adoption for mission critical workloads in this highly regulated sector.  The Council is comprised of four groups and corresponding forums:   * IT Council (CIO, CTO) * Security Council (CISO) * Risk Council (IT and Operations Risk Leaders) * Regulatory Outreach (Financial Industry Regulators)   Participation in the Council is by invitation only. |
| **Are there other financial institutions who have agreed to adopt the IBM Cloud for Financial Services™?** |
| Yes. Publicly disclosed collaborators have joined the Financial Council. Luminor (Baltics) recently signed an agreement to use IBM Cloud for Financial Services. Other FS Cloud wins include:   * Hamburg Commercial Bank (7M) * Lloyds (3M) * Broadridge (2M) * Legal & General (1M) * Nationwide Credit (1M)   For additional information:   * Luminor (Baltics) Press Release: <https://newsroom.ibm.com/2021-01-26-Luminor-Bank-Adopts-IBM-Cloud-for-Financial-Services-to-Accelerate-Digital-Transformation> |
| **What are IBM’s experiences / assets / accelerators in this space?** |
| * Hardened design from requirements based on the most security & compliance conscious global enterprises * IBM Promontory and IBM Security Services expertise spanning with experience working in over 75 jurisdictions and a detailed obligations library covering the specific requirements of 25 geographies (over 75 regulators) * Operational consistency across on-prem and IBM Cloud * Run mission critical VMware workloads on HA infrastructure * Right-size infrastructure, optimize performance and reduce TCO including no internal data bandwidth charges across IBM Private Network * Modernize VMware workloads with Red Hat OpenShift & PaaS across VMs and containers * Seamless integration and management providing automation-deployed solutions * Multiple consumption models both managed and unmanaged * World’s largest operator of VMware workloads * 100,000+ VMs migrated to the cloud without re-platforming or re-factoring * Deep expertise in highly regulated industry verticals and deep expertise in banking regulations with Promontory * Offload management of day-2 operations * Accelerate the client’s journey to cloud by leveraging IBM Services to help transform their IT * Run SAP workloads on SAP-certified servers with automated landscapes. IBM has more than 35,000 SAP-focused practitioners. IBM was the first to complete 100 S/4HANA implementations. IBM Cloud for VMware Solutions is the portfolio of choice for enterprise-scale SAP implementations and IBM is consistently recognized by VMware as a top cloud partner running the VMware Software Defined Data Center (SDDC) stack in data centers around the world.   References of clients using VMware on IBM Cloud today include several great references to start with:   * American Airlines: <https://www.ibm.com/case-studies/american-airlines> * Dream Payments: <https://www.ibm.com/case-studies/dream-payments-cloud> * Ricoh: <https://www.ibm.com/case-studies/ricoh-cloud-video-web-conferencing> * Osram: <https://www.ibm.com/case-studies/osram>   For additional information:   * SAP S/4HANA Running on Cloud: <https://www.ibm.com/cloud/blog/sap-s-4hana-running-on-cloud> |
| **What are the Service Level Agreements (SLA) for FS Cloud?** |
| The SLA for the FS Cloud are the same as for the IBM Public Cloud. IBM Cloud provides a 99.99% availability SLA.    The Availability SLA allows clients to receive a credit toward their account if they experience availability less than the 99.99%. Availability downtime is the total minutes they are unable to connect to any of their service instances. Total downtime minutes start when clients can prove a loss of availability with logs or any other records.  For additional information:   * Cloud Service Level Agreements: <https://cloud.ibm.com/docs/overview/terms-of-use?topic=overview-slas> |

# **Appendix A: Acronyms and Definitions**

|  |  |
| --- | --- |
| **Term** | **Definition** |
| **1H** | First Half (of the year noted) |
| **2H** | Second Half (of the year noted) |
| **Accelerator** | A tool, function, framework, defined process, industry / best practices that allow something of benefit to be delivered faster. Example: IBM Cloud for Financial Services™ with automated configurations allows the environment to be ready to accept data in two weeks which saves time and cost on the front-end and delivers business benefits sooner. |
| **Access Group** | A group of users and service IDs can be organized so that the same access can be assigned to all members within the group by using one or more policies. With access groups, clients can streamline the access assignment process so that they can manage a smaller number of policies and reduce the number of policies in an account, which in turn increases performance. After groups are set up, they can start assigning policies by selecting an access group as the subject of the policy. For more information, see “Setting up access groups”  Reference: <https://cloud.ibm.com/docs/account?topic=account-groups> |
| **Access policies** | Access policies are how users, service IDs, and access groups in the account are given permission to access and take actions on account resources. Policies include a subject, target, and role. The subject is the user, service ID, or access group that you are providing access. The target of the policy is the resource to which you want to provide access. And the IAM roles define the level of access or allowed actions on the target of the policy. |
| **Account Resources** | Account resources are the provisioned service offerings that are selected from the catalog or finer-grained resources within a service instance, such as an IBM® Cloud Object Storage bucket. IAM-enabled resources are added to a resource group when they are created from the catalog. |
| **Adobe** | IBM partner providing software support for the IBM Cloud for Financial Services™ capabilities   * Hybrid cloud: Adobe Experience Manager will be certified and delivered on Red Hat OpenShift, giving enterprises flexibility to host, access, and leverage their client data in the cloud environment of their choice. * For Regulated industries: IBM will enable Adobe Experience Manager (part of Adobe Experience Cloud) for professionals in the financial services market using the industry first IBM Cloud for Financial Services™.   Reference:   * Adobe: <https://www.adobe.com/> * Adobe & IBM Partnership: <https://w3.ibm.com/w3publisher/behind-the-news/adobe-partnership> |
| **Amberoon** | IBM partner providing agile compliance for AML. Reference: <https://www.amberoon.com/> |
| **API** | Application programming interface |
| **Aseria** | IBM partner providing AI cash flow advisor capabilities for SME for the IBM Cloud for Financial Services™ partner.  Reference: <https://www.asteria.ai/> |
| **Assima** | IBM partner providing solutions for remote user adoption for the IBM Cloud for Financial Services™  Reference: <https://assima.net/> |
| **ATracker** | IBM Cloud Activity Tracker, sometimes referred to as ATracker. Activity Tracker is a service to monitor the activity of their IBM Cloud account. I can be used to investigate abnormal activity and critical actions, comply with regulatory audit requirements, and provide alerts on actions as they happen. Events collected comply with the Cloud Auditing Data Federation (CADF) standard.  Reference: https://cloud.ibm.com/docs/Activity-Tracker-with-LogDNA?topic=Activity-Tracker-with-LogDNA-getting-started |
| **B2B** | Business to Business |
| **B2C** | Business to Consumer |
| **B2E** | Business-to-Employee |
| **Bastion Host** | A bastion host is a special-purpose computer on a network specifically designed and configured to withstand attacks. The computer generally hosts a single application, for example a proxy server, and all other services are removed or limited to reduce the threat to the computer. |
| **BCM** | Business Continuity Management |
| **BofA / BOA** | Bank of America |
| **BYOK** | Bring Your Own Key |
| **BYOL** | Bring Your Own License |
| **C3.ai** | IBM partner providing enterprise AI software provider for accelerating digital transformation. The proven C3 AI Suite provides comprehensive services to build enterprise-scale AI applications more efficiently and cost-effectively than alternative approaches.  Reference: <https://c3.ai/> |
| **CaaS** | Container as a Service |
| **CAGR** | Compound Annual Growth Rate |
| **CAS** | Cloud Advisory Services (IBM) |
| **Caveonix RiskForesight** | Continuous detection, prediction, and action on cyberthreats and regulatory compliance risks on hybrid clouds.  Reference: <https://www.caveonix.com/> |
| **CCO** | Chief Compliance Officer |
| **CEH** | Cloud Engagement Hub. The IBM Cloud Engagement Hub is a dedicated high-performance technical team to support strategic enterprise opportunities and create significant client value using IBM Public Cloud, RedHat, and Cloud Paks. The Cloud Engagement Hub works with financial services clients to define their respective cloud journeys based on existing IT landscape and investments. The Cloud Engagement Hub leads the solutioning for new cloud model deals defining client value, cloud architectures, migration / modernization journeys, target operating models, and execution strategy. |
| **CEO** | Chief Executive Officer |
| **CIO** | Chief Information Officer |
| **CISO** | Chief Information Security Officer |
| **Cloud Foundry** | Cloud Foundry ensures that the build and deploy aspects of coding remain carefully coordinated with any attached services — resulting in quick, consistent and reliable iterating of applications. As an industry-standard platform as a service (PaaS), Cloud Foundry ensures the fastest, easiest and most reliable deployment of cloud-native applications. IBM offers the Cloud Foundry PaaS in several hosting models, allowing clients to customize their PaaS experience and balance a range of considerations, including price, deployment speed and security.  Reference: <https://www.ibm.com/cloud/cloud-foundry?lnk=STW_US_STESCH&lnk2=learn_CloudFoundry&pexp=DEF&psrc=NONE&mhsrc=ibmsearch_a&mhq=cloud%20foundry> |
| **Co-location or CoLo** | A colocation (CoLo) is a data center facility in which a business can rent space for servers and other computing hardware. Typically, a CoLo provides the building, cooling, power, bandwidth and physical security while the client provides servers and storage. |
| **Containers** | Containers provide a standard way to package an application's code, configurations, and dependencies into a single unit that can run as a resource-isolated process on a compute server. To run an app in Kubernetes on Red Hat OpenShift on IBM Cloud, first containerize the app by creating a container image that is stored in a container registry. |
| **ContinuityLogic** | IBM partner providing a platform providing Business Continuity Management, Disaster Recovery Management, Incident Management, Crisis Management, Enterprise Risk Management, Vendor Risk Management, and Cybersecurity Reference: <https://www.continuitylogic.com/> |
| **CRN** | Cloud Resource Name: a Cloud Resource Name (CRN) uniquely identifies IBM Cloud® resources. A CRN is used to specify a resource in an unambiguous way that is guaranteed to be globally unique. A CRN is formed from a concatenation of "segments" that hierarchically identify the resource, its location, and the service it belongs to. The segment delimiter is set to a colon (:). All CRNs begin with the segment identifier crn. |
| **CRO** | Chief Risk Officer |
| **CSC** | Cloud Service Client |
| **CSE** | Cloud Service Endpoints (CSE) are automatically enabled for new VPCs, but VPCs that existed prior to the feature need to be updated to enable the feature. In a Virtual Private Cloud (VPC) on Classic created before 9 October 2019, the cloud service endpoints feature does not properly link endpoints. |
| **CSP** | Cloud Service Provider |
| **DC** | Data Center |
| **Decision Focus** | IBM partner providing governance, risk, and compliance (GRC) software.  Reference: <https://www.decisionfocus.com/> |
| **DEK** | Data Encrypted Key; an encryption key is typically a random string of bits generated specifically to scramble and unscramble data. Encryption keys are created with algorithms designed to ensure that each key is unique and unpredictable. The longer the key constructed this way, the harder it is to break the encryption code. |
| **Developer Tools** | Products that support developing, testing, and debugging software. |
| **DR** | Disaster Recovery |
| **DRY** | Don’t Repeat Yourself (DRY) is a principle of software development aimed at reducing repetition of software patterns, replacing it with abstractions or using data normalization to avoid redundancy. |
| **Enghouse Interactive** | Collaborative Contact Center software for Microsoft Teams.  Reference: <https://www.enghouseinteractive.com/> |
| **EU** | European Union |
| **Focal** | An IBM competency lead or subject matter expert (SME) able to provide deep support regarding a particular topic. A Focal may be able to provide resources to assist with projects or other efforts. |
| **Finacle** | Digital banking solution suite from EdgeVerve Systems, a subsidiary of Infosys. It provides frictionless client experiences, larger ecosystem play, insights-driven interactions and ubiquitous automation. Finacle solutions address the core banking, omnichannel banking, payments, treasury, origination, liquidity management, Islamic banking, wealth management, analytics, artificial intelligence, and blockchain requirements of financial institutions to drive business excellence.  Reference: [www.finacle.com](http://www.finacle.com) |
| **FIPS 140-2 Level 4** | Federal Information Processing Standard Publication 140-2. It is a U.S. government computer security standard used to approve cryptographic modules |
| **Fortinet** | IBM partner providing cybersecurity products and services, such as firewalls, anti-virus, intrusion prevention and endpoint security.  Reference: <https://www.fortinet.com/> |
| **FS** | Financial Services |
| **FS-ISAC** | Financial Services Information Sharing and Analysis Center; the only global cyber intelligence sharing community solely focused on financial services. Serving financial institutions and in turn their clients, the organization leverages its intelligence platform, resiliency resources, and a trusted peer-to-peer network of experts to anticipate, mitigate and respond to cyber threats.  Reference: https://www.fsisac.com/ |
| **FSS** | Financial Service Sector (IBM usage) |
| **GA** | General Availability (software release in general production) |
| **GBS** | IBM Global Business Services |
| **GDPR** | General Data Protection Regulation (EU) |
| **Geva Group** | Deep analytics in the field of chemistry. Reference: http://umich.edu/~gevalab/ |
| **GL** | Guidelines |
| **GP VPN** | Global Protect Virtual Private Network (GP VPN); the Global Protect VPN is a web browser-based VPN service, and should work with most browsers, operating systems, and mobile devices. All traffic on the browser tab that is used to log in to the service travels through an encrypted tunnel which terminates on the campus gateway. |
| **GSI** | Global Systems Integrator |
| **GTS** | IBM Global Technology Services |
| **HA** | High Availability |
| **Hamilton** | IBM Cloud for Financial Services™ |
| **HIPAA** | Health Insurance Portability and Accountability Act (US) |
| **HPCS** | Hyper Protect Crypto Services |
| **HSM** | Hardware Security Module |
| **Hybrid Cloud** | Hybrid Cloud is a composition of a public cloud and a private environment, such as a private cloud or on-premises resources, that remain distinct entities but are bound together, offering the benefits of multiple deployment models. Hybrid cloud can also mean the ability to connect collocation, managed and/or dedicated services with cloud resources. Gartner defines a hybrid cloud service as a cloud computing service that is composed of some combination of private, public and community cloud services, from different service providers. A hybrid cloud service crosses isolation and provider boundaries so that it can't be simply put in one category of private, public, or community cloud service. It allows one to extend either the capacity or the capability of a cloud service, by aggregation, integration or customization with another cloud service.  Varied use cases for hybrid cloud composition exist. For example, an organization may store sensitive client data in house on a private cloud application but interconnect that application to a business intelligence application provided on a public cloud as a software service. This example of hybrid cloud extends the capabilities of the enterprise to deliver a specific business service through the addition of externally available public cloud services. Hybrid cloud adoption depends on a number of factors such as data security and compliance requirements, level of control needed over data, and the applications an organization uses.  Another example of hybrid cloud is one where IT organizations use public cloud computing resources to meet temporary capacity needs that cannot be met by the private cloud. This capability enables hybrid clouds to employ cloud bursting for scaling across clouds. Cloud bursting is an application deployment model in which an application runs in a private cloud or data center and "bursts" to a public cloud when the demand for computing capacity increases. A primary advantage of cloud bursting and a hybrid cloud model is that an organization pays for extra compute resources only when they are needed. Cloud bursting enables data centers to create an in-house IT infrastructure that supports average workloads, and use cloud resources from public or private clouds, during spikes in processing demands. The specialized model of hybrid cloud, which is built atop heterogeneous hardware, is called "Cross-platform Hybrid Cloud". A cross-platform hybrid cloud is usually powered by different CPU architectures, for example, x86-64 and ARM, underneath. Users can transparently deploy and scale applications without knowledge of the cloud's hardware diversity. This kind of cloud emerges from the rise of ARM-based system-on-chip for server-class computing.  Hybrid cloud infrastructure essentially serves to eliminate limitations inherent to the multi-access relay characteristics of private cloud networking. The advantages include enhanced runtime flexibility and adaptive memory processing unique to virtualized interface models. |
| **HyTrust Data Control w/HPCS** | Strong encryption with integrated key management to secure workloads throughout their lifecycle.  Reference: <https://www.hytrust.com/datacontrol-ibm-cloud/> |
| **IaaS** | Infrastructure as a service |
| **IBM** | International Business Machines |
| **IBM Cloud for Financial Services™ Validated** | Name is used to designate an IBM Cloud service or ecosystem (ISV, SaaS) partner service is IBM Cloud for Financial Services™ validated and has evidenced compliance to IBM Cloud Framework for Financial Services controls, architecture and operations requirements |
| **IBM Privacy Shield Policy for IBM Cloud Services** | The IBM Privacy Shield Privacy Policy for Cloud Services (the “Policy”) applies to the IBM Infrastructure-as-a-Service, Platform-as-a-Service, Software-as-a-Service, and other hosted offerings that are Privacy Shield certified (“Privacy Shield-Certified Cloud Services”). A list of these offerings is [provided below](https://www.ibm.com/privacy/privacy-shield#shield_offerings); if an offering is not on this list, it is not covered by the IBM Privacy Shield.  As the Privacy Shield only applies to personal data transferred to the United States from those countries whose data protection laws recognize Privacy Shield as a valid mechanism for such cross-border transfers, this Statement only applies to:   1. such personal data hosted in the United States through the Privacy Shield-Certified Cloud Services; and 2. select offerings when the data is hosted outside the United States but the Cloud Service processing is temporarily directed to a United States data center to enable continued availability and resiliency.   This Policy does not otherwise apply when clients choose to have their offering content hosted in other countries.  Reference: <https://www.ibm.com/privacy/privacy-shield> and  To learn more about the Privacy Shield Program, or to view the certification applicable to certain IBM Cloud Services, please visit [www.privacyshield.gov](https://www.privacyshield.gov/welcome). |
| **IBM Promontory** | A subsidiary of IBM and global consulting firm advising clients on regulatory issues, compliance, risk management, liquidity, restructuring, acquisitions, due diligence, internal investigations and cyber security. |
| **IBM Security** | Supported by IBM X-Force research, the group offers enterprise security products and services monitoring 70 billion security events per day in more than 130 countries and has more than 10,000 security patents worldwide. |
| **IBM Virtual Server Infrastructure (VSI)  transient servers** | Ideal for the development and testing of applications and other nonproduction workloads that don’t require constant uptime, transient servers are deprovisioned on a first-on, first-off basis. |
| **IBM Virtual Server Infrastructure (VSI) dedicated hosts** | Single tenant dedicated hosts help control workload placement and support network throughputs of up to 20 Gbps. View core, RAM and local storage consumption for maximum control of workload management. |
| **IBM Virtual Server Infrastructure (VSI) dedicated servers** | Take full advantage of our single tenant offering with rapid provisioning for further control and flexibility in VSI deployments, up to 56 cores and 484 GB RAM and monthly or hourly options. |
| **IBM Virtual Server Infrastructure (VSI) public servers** | Choose options for (1) a balance of performance and scale, (2) high I/O and low-latency performance, (3) CPU-intensive workloads, (4) memory-intensive workloads or (5) accelerated computing workloads. |
| **IBM Virtual Server Infrastructure (VSI) reserved servers** | Ideal for sustained workloads and enterprise-level challenges, a set of up to 20 VMs can be reserved in advance for guaranteed capacity in the data center of the clients choice. Choose a 1- or 3-year term. |
| **IC4V** | IBM Cloud for VMware Solutions |
| **IDP** | Identity Provider (IDP) |
| **IKS** | IBM Cloud Kubernetes Service |
| **Integration** | Products that facilitate the connection of data, apps, APIs, and devices across an organization to be more efficient, productive, and agile. |
| **Intellect** | IBM partner providing front, middle, and back-office platforms supporting corporate banking, retail banking, risk, treasury & capital, insurance, and digital solutions markets.  Reference: <https://www.intellectdesign.com/> |
| **Intercope** | IBM partner providing platforms for interbank messaging including multi-network connectivity, SWIFT CSP compliance, ISO 20022 migration, T2 & T2S consolidation supporting ESMIG, SWIFT gpi, Instant Payments for multiple CSMs over multiple networks, to legacy SWIFT consolidation and replacement.  Reference: [www.intercope.com](http://www.intercope.com) |
| **Internet of Things** | Products that support receiving and transferring data over wireless networks without human intervention. |
| **Internet Protocol Security (IPsec)** | Internet Protocol Security is a secure network protocol suite that authenticates and encrypts the packets of data to provide secure encrypted communication between two computers over an Internet Protocol network. It is used in virtual private networks. |
| **ISO 9001** | ISO 9001 defines a [Quality Management System (QMS)](https://the9000store.com/iso-9001-2015-requirements/what-is-iso-9001-quality-management-system/) allowing evaluation of whether an organization’s [quality management system](https://the9000store.com/iso-9001-2015-requirements/what-is-iso-9001-quality-management-system/) is appropriate and effective, while directing them to identify and implement improvements. ISO 9001 is the only standard in the 9000 series that requires certification  Reference: https://www.iso.org/iso-9001-quality-management.html |
| **ISO 27001** | ISO 27001 is an international standard on how to manage information security. The standard was originally published jointly by the International Organization for Standardization and the International Electrotechnical Commission in 2005 and then revised in 2013.  Reference: https://www.iso.org/standard/54534.html |
| **ISO 27017** | ISO 27017 is a security standard developed for cloud service providers and users to make a safer cloud-based environment and reduce the risk of security problems.  Reference: https://www.iso.org/standard/43757.html |
| **ISO 27018** | ISO 27018 is a security standard and part of the ISO 27000 family of standards. It was the first international standard about the privacy in [cloud computing](https://en.wikipedia.org/wiki/Cloud_computing) services which was promoted by the industry. Created in 2014, it helps cloud service providers who process [personally identifiable information](https://en.wikipedia.org/wiki/Personally_identifiable_information) (PII) to assess risk and implement controls for protecting PII. It was published by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) under the joint ISO and IEC subcommittee.  Reference: https://www.iso.org/standard/61498.html |
| **ISV** | Independent Service Vendor |
| **IT** | Information Technology |
| **Key Management Interoperability Protocol (KMIP)** | The Key Management Interoperability Protocol (KMIP) is an extensible communication protocol that defines message formats for the manipulation of cryptographic keys on a key management server. This facilitates data encryption by simplifying encryption key management. |
| **Knowis** | IBM partner providing banks with pre-integrated independent technologies on shared, ontology-based domain models on IBM’s Smarter Process Technology.  Reference: [www.knowis.com](http://www.knowis.com) |
| **Kubernetes** | Kubernetes is an open-source platform for managing containerized workloads and services across multiple hosts, and offers management tools for deploying, automating, monitoring, and scaling containerized apps with minimal to no manual intervention. |
| **KYOK** | Keep Your Own Key |
| **Line of Shared Responsibility (LoSR)** | Found within the Shared Responsibility Model, the Line of Shared Responsibility defines the border between security responsibilities in cloud environments. Those areas, domains, platforms, etc. above the Line of Shared responsibility are the responsibility of the client. Those areas, domains, platforms, etc. below the Line of Shared responsibility are the responsibility of the Cloud Service Provider. |
| **Logging and Monitoring** | Products that support storing, searching, analyzing, and monitoring log data and events. And products that support reviewing and managing the operational workflow and processes being logged. |
| **Lumina** | IBM partner providing development in partnership with IBM. Reference: www.luminacorp.com |
| **Mobile** | Products with specific or special utility for users creating things to be used on mobile devices. |
| **MQ** | IBM MQ or IBM Message Queue; MQ (message queue) series, is an IBM standard for program-to-program messaging across multiple platforms. MQ is sometimes referred to as message-oriented middleware (MOM) |
| **MTCS – Level 3** | Multi-Tier Cloud Security (MTCS) is an information security standard, published by [Singapore Standards](https://en.wikipedia.org/wiki/Singapore_Standard_(regulatory_policy)). MTCS Singapore Standard (SS) 584 is the world’s first cloud security standard that covers multiple tiers of cloud security. The standard was last revised in 2015. SS 584 specifies a [Management system](https://en.wikipedia.org/wiki/Management_system) for Cloud Security, to three levels. Organizations that meet the requirements may be certified by an accredited certification body following successful completion of an [audit](https://en.wikipedia.org/wiki/Audit).  IBM is an MTCS Level-3 Certified Partner for IBM Cloud using IaaS model that spans across products such as bare metal servers, virtual servers (Private and Public), hardware security modules, and VMware vSphere on IBM Cloud. |
| **MVP** | Minimum Viable Product. It is a version of a product with just enough features to satisfy early clients and provide feedback for future product development. |
| **MZR** | Multi-Zone Region: if you create a cluster in a multizone metro location, the replicas of your highly available Kubernetes master are automatically spread across zones. You have the option to spread your worker nodes across zones to protect your apps from a zone failure. To determine whether a zone is multizone-capable, run ibmcloud ks locations and look for the value in the Multizone Metro column.  Reference: <https://cloud.ibm.com/docs/containers?topic=containers-regions-and-zones> |
| **NCA** | National Competent Authority. A medicines regulatory authority in a European Union Member State. |
| **Networking** | Products that support or augment the linking of computers so they can operate interactively. |
| **Network Access Control List (NACL)** | A network access control list (ACL) is an optional layer of security for a VPC that acts as a firewall for controlling traffic in and out of one or more subnets. A network ACL may be set up with rules similar to the security groups in order to add an additional layer of security to the Virtual Private Cloud (VPC). |
| **NexJ** | IBM partner providing intelligent client management for financial services organizations.  [Reference: www.nexj.com](http://Reference:%20%20www.nexj.com%20) |
| **OM** | IBM Offering Management |
| **OS** | Operating System or OpenShift (RedHat product) |
| **P2B** | Peer-to-Business |
| **P2P** | Peer-to-Peer |
| **PaaS** | Platform as a Service |
| **Para** | Paragraph |
| **PCI / PCI-DSS** | Payment Card Industry Data Security Standard. It is an information security standard for organizations that handle branded credit cards from the major card schemes. The PCI Standard is mandated by the card brands but administered by the Payment Card Industry Security Standards Council.  Reference: https://www.pcisecuritystandards.org/pci\_security/ |
| **Persistent** | IBM partner providing software design and development platforms.  Reference: [www.persistent.com](http://www.persistent.com) |
| **PING Identity** | Ping Identity is and enterprise intelligent identity solution enabling Zero Trust identity-defined security and more personalized, streamlined user experiences. The Ping Intelligent Identity™ platform provides clients, workforce, and partners with access to cloud, mobile, SaaS and on-premises applications across the hybrid enterprise. PingIdentity provides flexible identity solutions that accelerate digital business initiatives, delight clients, and secure the enterprise through multi-factor authentication, single sign-on, access management, intelligent API security, directory, and data governance capabilities. URL: https://www.pingidentity.com/en.html |
| **POAP** | Power On Auto Provisioning (POAP) automates the process of upgrading software images and installing configuration files on Cisco MDS and Nexus switches that are being deployed in the network. When a Cisco MDS switch with the POAP feature boots and does not find the startup configuration, the switch enters POAP mode, locates the DCNM DHCP server, and bootstraps itself with its interface IP address, gateway, and DCNM DNS server IP addresses. It also obtains the IP address of the DCNM server to download the configuration script that is run on the switch to download and install the appropriate software image and device configuration file. |
| **Public Cloud** | Cloud services are considered "public" when they are delivered over the public Internet, and they may be offered as a paid subscription, or free of charge.[100] Architecturally, there are few differences between public- and private-cloud services, but security concerns increase substantially when services (applications, storage, and other resources) are shared by multiple clients. Most public-cloud providers offer direct-connection services that allow clients to securely link their legacy data centers to their cloud-resident applications.  Several factors like the functionality of the solutions, cost, integrational and organizational aspects as well as safety & security are influencing the decision of enterprises and organizations to choose a public cloud or on-premise solution. |
| **Public-Private Hybrid Cloud** | A hybrid cloud is a model in which a private cloud connects with public cloud infrastructure, allowing an organization to orchestrate workloads across the two environments. In this model, the public cloud effectively becomes an extension of the private cloud to form a single, uniform cloud. |
| **Red Hat OpenShift AI/ML on OpenShift** | Red Hat OpenShift capability providing better collaboration between data scientists and software developers and accelerates the roll out of intelligent applications across hybrid cloud. |
| **Red Hat OpenShift Databases and data analytics** | Red Hat OpenShift capability providing methods for ingesting, storing, processing, and analyzing datasets from a variety of sources for use cases such as mobile and ecommerce applications, AI/ML, business intelligence, and more. |
| **Red Hat OpenShift Edge computing** | Red Hat OpenShift capability providing 3-node clusters as well as remote worker nodes to provide organizations full Kubernetes capabilities in a smaller footprint. |
| **Red Hat OpenShift on IBM Cloud** | Red Hat OpenShift on IBM Cloud is a managed offering to create your own OpenShift cluster of compute hosts to deploy and manage containerized apps on IBM Cloud. Red Hat OpenShift on IBM Cloud provides intelligent scheduling, self-healing, horizontal scaling, service discovery and load balancing, automated rollouts and rollbacks, and secret and configuration management for your apps. Combined with an intuitive user experience, built-in security and isolation, and advanced tools to secure, manage, and monitor your cluster workloads, you can rapidly deliver highly available and secure containerized apps in the public cloud. |
| **Red Hat OpenShift Operators** | Red Hat OpenShift capability providing automated installation, upgrades, and life-cycle management for every part of your container stack, providing a more secure and up-to-date Kubernetes application platform with no downtime. |
| **Red Hat OpenShift Pipelines** | Red Hat OpenShift capability providing a streamlined user experience through the OpenShift console developer perspective, command-line interfaces (CLIs), and integrated development environments (IDEs). |
| **Red Hat OpenShift Serverless** | Red Hat OpenShift capability providing a uniform way to manage, connect, and observe applications as managing and security between services becomes more difficult.  an application to use compute resources and automatically scale up or down based on use, driven on-demand from a number of event sources. |
| **Red Hat OpenShift Service Mesh** | Red Hat OpenShift capability providing a uniform way to manage, connect, and observe applications as managing and security between services becomes more difficult. |
| **Red Hat OpenShift Virtualization** | Red Hat OpenShift capability providing virtual machines to OpenShift to modernize existing applications or run them alongside containers, and serverless, in a Kubernetes-native architecture. |
| **Red Hat VPC Clusters** | Red Hat VPC Clusters are created in your own Virtual Private Cloud providing the security of a private cloud environment with the dynamic scalability of a public cloud. Network access control lists are used to protect the subnets to which the worker nodes are connected. VPC clusters can be provisioned on shared virtual infrastructure only. |
| **RH** | Red Hat |
| **RHEL** | Red Hat Enterprise Linux |
| **Ripe Hub** | IBM partner providing frictionless payments ecosystem. Reference: [www.ripehub.com](http://www.ripehub.com) |
| **Robust Intelligence** | IBM partner providing secure deployment of Artificial Intelligence (AI) to financial institutions, online payment processors, and government agencies. Reference: [robustintelligence.com](https://www.robustintelligence.com/) |
| **ROKS** | Red Hat OpenShift on IBM Cloud |
| **SaaS** | Software as a Service |
| **Security** | Products that provide the protection of stored data from theft, leakage, and deletion. |
| **SIEM** | Security Information and Event Management (SEIM) is within the field of computer security where software products and services combine security information management and security event management. They provide real-time analysis of security alerts generated by applications and network hardware. |
|  |  |
| **Service ID** | A service ID identifies a service or application similar to how a user ID identifies a user. A service ID that you create can be used to enable an application outside of IBM Cloud access to your IBM Cloud services. You can assign specific access policies to the service ID that restrict permissions for using specific services, or even combine permissions for accessing different services. Since service IDs are not tied to a specific user, if a user happens to leave an organization and is deleted from the account, the service ID remains ensuring that your application or service stays up and running. |
| **Shared Responsibility Model** | Found within the Shared Responsibility Model, theLine of Shared Responsibility defines the border defining the security responsibilities in cloud environments for the client or the Cloud Service Provider. Those areas, domains, platforms, etc. that are above the Line of Shared responsibility are owned by the client. Those areas, domains, platforms, etc. below the Line of Shared responsibility are owned by the Cloud Service Provider. |
| **Shield** | IBM partner providing anti-fraud solutions.  Reference: [www.shield.com](http://www.shield.com) |
| **SLA** | Service Level Agreement |
| **SOA** | Services Oriented Architecture |
| **SOC 1** | SOC 1 is a report on controls at a service organization relevant to a user entity's internal control over financial reporting |
| **SOC 2** | SOC 2 is a report on controls at a service organization relevant to security, availability, processing integrity, confidentiality, or privacy. |
| **SOC 3** | SOC 3 is a trust services report for service organizations. |
| **SOCx** | Service Organization Control (including all SOC reports / processes SOC 1, SOC 2, SOC 3) |
| **Spanugo** | IBM acquisition providing cybersecurity assurance for the hybrid cloud; spanugo.com;  Reference: IBM acquisition announcement: <https://newsroom.ibm.com/2020-06-15-IBM-Acquires-Assets-from-Spanugo> |
| **SRE** | Site Reliability Engineering (SRE) is a discipline that incorporates aspects of software engineering and applies them to infrastructure and operations problems. The main goals are to create scalable and highly reliable software systems. |
| **Storage** | Products that support data to be created, read, updated, and deleted. |
| **SunTec** | IBM partner providing open banking platforms.  Reference: [www.suntecgroup.com](http://www.suntecgroup.com) |
| **SZR** | Single-Zone Region; If you create a cluster in a single zone (data center) location, you can create multiple worker nodes, but you cannot spread them across zones. The highly available master includes three replicas on separate hosts but is not spread across zones.  Reference: <https://cloud.ibm.com/docs/containers?topic=containers-regions-and-zones> |
| **TCA** | Technology Compliance Advisor. It is an IBM subscription service providing regulatory updates, impact analysis, and alignment to a client’s regulatory technology controls.  Reference: |
| **TCO** | Total Cost of Ownership |
| **Tekton** | Tekton is a flexible open-source framework for creating CI / CD systems, allowing developers to build, test, and deploy across cloud providers and on-premise systems.  Reference: <https://tekton.dev/> |
| **Temenos** | IBM partner providing cloud-native, cloud-agnostic, API-first digital banking, core banking, payments, fund management, and wealth management software products.  Reference: [www.temenos.com](http://www.temenos.com) |
| **Terraform** | Terraform is an open-source infrastructure as code software tool that provides a consistent CLI workflow to manage hundreds of cloud services. Terraform codifies cloud APIs into declarative configuration files.  Reference: <https://www.terraform.io/> |
| **Thought Machine** | IBM partner providing cloud native core banking platforms. Reference: [thoughtmachine.net](https://thoughtmachine.net/) |
| **TickTrade** | IBM partner providing intelligent foreign exchange (FX) trading, payments and analytics platforms.  Reference: [www.ticktradesystems.com](http://www.ticktradesystems.com) |
| **TLS** | Transport Layer Security; a cryptographic protocol designed to provide communications security over a computer network |
| **UI** | User Interface |
| **US** | United States |
| **VCS** | Veritas Cluster Server (rebranded as Veritas Infoscale Availability but also known as VCS) is a high-availability cluster software for Unix, Linux and Microsoft Windows computer systems, created by Veritas Technologies. It provides application cluster capabilities to systems running other applications, including databases, network file sharing, and electronic commerce websites. |
| **Veeam** | IBM partner providing backup and replication for cloud, virtual and physical workloads. Suggested for IBM Cloud for Financial Services™ backup. Reference: <https://www.veeam.com/> |
| **Veeam Data Mover Services** | Veeam Data Mover Service is a component that gives access to a host by enabling Veeam Data Movers – agents that are responsible for VM data processing and transfer.  Reference: https://helpcenter.veeam.com/docs/backup/vsphere/veeam\_transport\_service.html?ver=110 |
| **Vermeg** | IBM partner providing financial software including securities processing software and fund administration systems. Reference: [www.vermeg.com](http://www.vermeg.com/) |
| **Virtual Private Cloud (VPC)** | A virtual private cloud is an on-demand configurable pool of shared resources allocated within a public cloud environment, providing a certain level of isolation between the different organizations using the resources. |
| **VMS** | Virtual Machine System; a virtual machine that provides a complete system platform and supports the execution of a complete operating system (OS) |
| **VMW** | VMware. Reference: <https://www.vmware.com/> |
| **VPC** | A Virtual Private Cloud (VPC) is a public cloud offering that lets an enterprise establish its own private cloud-like computing environment on shared public cloud infrastructure. A VPC gives an enterprise the ability to define and control a virtual network that is logically isolated from all other public cloud tenants, creating a private, secure place on the public cloud. |
| **VPC** | Virtual Private Cloud |
| **vRealize Network Insight** | VMware offering; an optimized, highly available and secure network infrastructure across hybrid and multicloud environments |
| **vSAN** | Enterprise-class, storage virtualization software creating a virtual storage area network, a collection of ports from a set of connected fibre channel switches, that form a virtual fabric. Ports within a single switch can be partitioned into multiple VSANs, despite sharing hardware resources. |
| **VSI** | Virtual Server Infrastructure |
| **WW** | World-wide |
| **WDEK** | Wrapped Data Encryption Key; Key Wrap constructions are a class of symmetric encryption algorithms designed to encapsulate (encrypt) cryptographic key material. The Key Wrap algorithms are intended for applications such as protecting keys while in untrusted storage or transmitting keys over untrusted communications networks. The constructions are typically built from standard primitives such as block ciphers and cryptographic hash functions. |
| **Z** | IBM mainframe enterprise platform for mission-critical applications |
| **Zafin** | IBM partner providing relationship-based pricing to banks and financial institutions.  Reference: [www.zafin.com](http://www.zafin.com) |
| **Zerto** | An IT resilience platform, converging disaster recovery, backup and cloud mobility in one simple, scalable platform. Recommended for disaster recovery for IBM Cloud for Financial Services™  Reference: <https://www.zerto.com/> |