Key considerations when choosing cloud services in financial services

Cloud services can help financial services firms achieve their digital innovation goals more quickly and effectively.

This overview discusses seven key areas of consideration when moving to the cloud and selecting a cloud service:

- Service policies, procedures, and plans
- Operations management
- Security and compliance
- Identity and access management
- Incident management
- Disaster recovery
- Change management

facebook.com/redhatinc
@RedHat
linkedin.com/company/red-hat

Hybrid cloud is essential for achieving business priorities and regulatory compliance

Across industries, hybrid cloud adoption is growing. In fact, 81% of financial services firms say that the cloud is the most essential technology for achieving business priorities, and 74% have adopted a cloud-first approach for new application development.[1] Cloud-native technologies like Kubernetes and containers play key roles in hybrid cloud environments. They support efficient, agile ways for developing, deploying, and consuming business applications and services across on-site, cloud, and edge infrastructure. They can also help financial services firms address evolving regulatory requirements, shifting customer preferences, and new competition more easily.

Even so, building and maintaining a hybrid cloud infrastructure and container application platform in-house can be challenging and time consuming. You must reassess how you perform common IT operations and manage ongoing security and compliance tasks, as well as develop your staff's skills and expertise. You also need to consider how both existing and proposed regulatory requirements will apply to your new environment to ensure compliance. Finally, because financial services firms use an average of three public clouds in addition to privately operated infrastructure,[1] you must understand how to connect and operate all of your environments consistently.

Adopting one or more managed cloud services can help you overcome this complexity and achieve your goals more quickly. Managed cloud services can simplify deployment, streamline operations, and speed time to value compared to in-house solutions. A third party builds, manages, and operates cloud infrastructure for you, providing access to the application platform and allowing your teams to focus on business priorities.

Deploying a consistent hybrid cloud application platform—like Red Hat® OpenShift®—across your infrastructure can further simplify your operations while increasing security, easing compliance, and improving application portability. Red Hat works with key cloud provider partners to deliver fully managed Red Hat OpenShift cloud services to help you accelerate your journey to the cloud.

Key considerations for choosing cloud services in highly regulated industries

While cloud services can deliver many benefits, they do require changes to the way your organization approaches operations, security, and compliance. At the core of these changes is the *shared responsibility model*. A shared responsibility model dictates which tasks and actions your cloud service provider addresses, and which your own organization must address. It's important to understand that while using cloud services transfers many *tasks* to your service provider, in the eyes of regulators, your organization still remains responsible for *all risks* associated with the cloud service.

[1] Frost & Sullivan. "Optimizing Your Cloud Strategy to Meet Business Goals," December 2022.

Achieve more for less

Read this brief to learn how Red Hat OpenShift cloud services can help you save time and money.

Security and compliance are typically the key concerns in shared responsibility models, but these models often extend to broader IT controls and operations. For example, your cloud service provider may be tasked with ensuring cloud infrastructure is configured according to security best practices while you may be tasked with managing your data and its protections. And some controls, like patching, may be shared – your cloud service provider must patch the underlying infrastructure while you must patch the operating systems and applications running in your cloud service.

The following sections review the operational impact of adopting cloud services for financial services in several key areas and discuss considerations for selecting a cloud service provider.

Our take: Red Hat OpenShift cloud services provide documented, regularly-reviewed policies, procedures, and plans to help you understand the scope of the service offering and how tasks and incidents are handled.

Service policies, procedures, and plans

Your organization operates according to approved policies, procedures, and plans to ensure that everything runs as expected over time, and that incidents are dealt with in a predetermined manner. Your cloud service provider will handle many of these elements. It's important to understand your cloud service provider's policies, procedures, and plans for all operations that they cover – including operations management, security and compliance, identity and access management, incident management, disaster recovery, and change management.

When choosing a cloud services provider, look for:

- Detailed documentation of responsibilities, actions, and roles.
- Regular reviews, assessments, and approvals of all necessary documentation.
- Documentation coverage for all operations within the cloud service offering.

You should also be sure that your cloud service provider's policies, procedures, and plans align with your organization's needs.

Our take: Red Hat OpenShift cloud services provide documented operational management plans and processes to establish policies, expectations, and roles for day-to-day operations. Formal vendor management policies and review processes address risks related to third-party vendors. Automation is broadly employed for installation, scaling, and on-demand changes while real-time monitoring and logging track events.

Operations management

Your cloud service provider will manage day-to-day operations for your cloud infrastructure according to detailed service level agreements (SLAs). Ensuring that these SLAs meet your organization's requirements is key. It's also important to understand how your cloud service provider manages their own service providers, as the associated operational risk will impact your organization.

Look for:

- **Detailed documentation about your cloud service provider's governance model as it applies to third-party services included within the cloud service.** Ensure that related operational risks are managed in a consistent and effective manner that aligns with your own governance model.
- **Real-time monitoring of the performance and availability of the constituent services that make up the cloud service.** Monitoring and logging should be a key part of ensuring that SLAs are met. Log data should be protected and made available to your organization and designated regulators as requested for auditing and investigation purposes.
- **Detailed documentation about performance and capacity planning.** Roles and responsibilities – and how they relate to your cloud provider's shared responsibility model – should be specified in detail.

Security and compliance

Our take: Red Hat OpenShift cloud services are certified to key standards – including Payment Card Industry Data Security Standard (PCI DSS), System and Organization Controls (SOC) 2, and International Organization for Standardization (ISO) 27001 – to help protect against threats.

Security and compliance are ongoing concerns for all organizations, especially financial institutions. Many shared responsibility models focus on security and compliance, but your organization is ultimately still responsible for all risks. Ensuring that your cloud service complies with all corporate, industry, and government security regulations is critical.

Look for:

- Detailed documentation of the shared responsibility model that defines which organization is responsible for each task and clearly delineates responsibility and expectations for shared tasks like network security and vulnerability management.
- Regular, structured reassessment and adaptation of security and compliance controls, including any operated by third parties.
- Certification to all industry and government standards that apply to your organization.
- Client audit capabilities, including the ability to grant access to key information for client and regulators to support supervisory needs.

Identity and access management

Our take: Red Hat OpenShift cloud services employ identity and access management best practices – including least privileges, RBAC, multifactor authentication (MFA), and real-time monitoring and logging – throughout the cloud stack.

Identity and access management (IAM) is a critical part of any operational framework. Much as your organization maintains IAM systems within your own datacenter, your cloud service provider will operate an IAM system for your cloud infrastructure. This IAM system and related processes must align with your organization's requirements as well as all relevant regulations. In addition, zero trust architectures can provide increased protection for your cloud environment and should be considered both for your cloud service and your overall organization.

When considering cloud services, look for:

- Detailed role-based access controls (RBAC) for your cloud service.
- Use of least privilege and segregation of duties principles for all roles.
- Monitoring to ensure ongoing compliance with access controls and requirements.
- Periodic assessment and recertification of elevated and privileged access.
- Logging of actions for all privileged accounts for traceability in investigations.
- Integration with your existing IAM systems.

Our take: Red Hat OpenShift cloud services provide documented incident response plans and processes to describe how events are handled and communicated. Real-time monitoring and logging capabilities identify and track incidents and notify appropriate parties.

Incident management

Even with the best-laid plans and controls, security, data protection, and availability incidents will occur. Your cloud service provider will be the first responder to incidents concerning your cloud service, but you may also need to take investigative action after the initial response. It's important to understand how your cloud service provider approaches and handles incidents.

Look for:

- A detailed triage approach and incident classification scheme.
- Monitoring and logging capabilities, with access to logs and information for roles within your organization as needed to investigate incidents.
- Timely, tested communications with your organization, regulators, and other authorized parties regarding potential incidents.
- Incident documentation to support forensic investigations and evidence gathering.
- Regular incident management process and response plan testing and reassessment.

Our take: Red Hat OpenShift cloud services provide documented disaster recovery plans and processes to describe how incidents are handled and communicated.

Disaster recovery

Financial services institutions offer critical services that must be available at all times—large-scale and extended outages are unacceptable. Even so, failures and incidents can occur – well-documented, tested, and validated disaster recovery plans are essential and often required to comply with industry regulations. When adopting a cloud service, you'll need to adapt your disaster recovery plans accordingly – understanding how your cloud service provider handles resiliency and recovery is critical.

Look for:

- Detailed resiliency and disaster recovery plans for all service components, client data, and third-party components.
- Regular, structured plan reassessment, testing, validation, and adaptation.
- Specifications for measuring constituent service availability and recovery time and how each impacts overall service availability.

Cloud service providers often handle service resiliency through staff co-location and geographically isolated cloud regions. It's important to understand where applications, data, and services may be moved or located during a disaster recovery situation to ensure you comply with data residency requirements.

Change management

Modern IT environments are dynamic and changes – whether due to updates, emerging regulatory issues, organizational shifts, or other events – are inevitable. As a result, every organization needs clear, traceable change management processes. When adopting a cloud service, your service provider will perform many changes – like updates, bug fixes, and security patching – for your organization. It's critical to understand your cloud service provider's change management process and ensure that it complies with your own policies and industry standards.

Look for:

- Detailed change management documentation, including processes for both standard changes like planned updates and emergency changes like zero day vulnerabilities.
- Formal change testing and validation systems to ensure changes do not negatively impact operations.
- Regular scanning, triage, and remediation of infrastructure for misconfigurations, security vulnerabilities, and compliance.
- Clear explanations of key stakeholders and how they are engaged for different types of changes.

Our take: Red Hat OpenShift cloud services provide documented change management procedures. A team assesses each change for potential impacts before moving forward and communicates information as appropriate. Changes are analyzed, tested, and deployed using an Agile methodology.

Why choose Red Hat OpenShift cloud services?

Optimized to improve developer productivity and promote innovation, Red Hat OpenShift is an enterprise-ready Kubernetes container platform with full-stack automated operations for managing hybrid cloud, multicloud, and edge deployments. Red Hat OpenShift cloud services are an ideal solution for financial services firms that want to move rapidly to the cloud while focusing on their core competencies. Red Hat works with key cloud provider partners to deliver fully managed container environment services that simplify deployment and operations while saving costs over in-house construction. With flexible pricing models, these services help you reduce support costs, increase operational efficiency, and free your staff to innovate.

Multiple Red Hat OpenShift cloud services are available, so you can choose the option that best fits your organization's needs:

- Red Hat OpenShift Dedicated, running on AWS or Google Cloud
- Red Hat OpenShift Service on AWS
- Microsoft Azure Red Hat OpenShift
- Red Hat OpenShift on IBM Cloud

Each service offers more than just access to managed software and technologies. They provide complete, full-stack environments with all necessary services, simple self-service options, and expert 24x7 support via stringent SLAs.

Key features

- Expert 24x7 support with at least 99.95% availability
- Proactive monitoring and preventative remediation action
- Always-on user portals with defined response times
- Access to a global team of expert engineering and support staff

Proven business benefits

Red Hat OpenShift cloud services also deliver proven business benefits:

- Shorten development cycles by up to 70%.[2]
- Recapture 20% of developer time from infrastructure maintenance work.[2]
- Improve operational efficiency by 50%.[2]
- Increase developer satisfaction and retention.[2]
- Increase security, reliability, and business continuity.[2]

Read the analyst study to learn more.

Learn more

Hybrid cloud environments are essential for success in today's highly competitive financial services market. Managed cloud services can help your organization adopt hybrid and multicloud environments rapidly and efficiently. Red Hat OpenShift cloud services simplify deployment and operations while saving costs and giving you a consistent application platform across on-site, cloud, and edge infrastructure. Learn more at redhat.com/fsi.

[2] Forrester Consulting study, commissioned by Red Hat. "The Total Economic Impact™ of Red Hat OpenShift Cloud Services," January 2022. Results are for a composite organization representative of interviewed customers..

About Red Hat

Red Hat is the world's leading provider of enterprise open source software solutions, using a community-powered approach to deliver reliable and high-performing Linux, hybrid cloud, container, and Kubernetes technologies. Red Hat helps customers develop cloud-native applications, integrate existing and new IT applications, and automate and manage complex environments. A trusted adviser to the Fortune 500, Red Hat provides award-winning support, training, and consulting services that bring the benefits of open innovation to any industry. Red Hat is a connective hub in a global network of enterprises, partners, and communities, helping organizations grow, transform, and prepare for the digital future.

North America	Europe, Middle East, and Africa	Asia Pacific	Latin America
1 888 REDHAT1	00800 7334 2835	+65 6490 4200	+54 11 4329 7300
www.redhat.com	europe@redhat.com	apac@redhat.com	info-latam@redhat.com

facebook.com/redhatinc
@RedHat
linkedin.com/company/red-hat