Crowe

Exploring the cloud

A guide to a secure, successful rollout

Transitioning to the cloud is a critical milestone in any financial services organization's digital transformation journey.

While navigating a cloud rollout, it's essential to build a strategy, proceed with care, and always keep the customer at the heart of the process.

1 Cloud computing in the financial services industry: An overview

Cloud computing has sparked radical change in various business sectors, and the financial services industry is no exception. Organizations are turning to the cloud so they can realize benefits such as improved operational efficiency, enhanced customer service, and a platform for innovative solutions. According to a 2022 Arzient/American Banker *survey*, 40% of respondents listed cloud computing as a top-five 2023 spending priority, and eight out of 10 expect to have at least 20% of their computing in the cloud this year.

Breaking down cloud models

Three primary cloud models exist, each with its unique set of advantages and potential challenges. Financial services organizations that want to adopt cloud computing should assess their specific requirements, their regulatory requirements, and the nature of the data they handle and then choose a cloud model that represents the best fit.

Following is a breakdown of three cloud models and their pros and cons.

Public cloud

The public cloud delivers services over the internet that are shared among various organizations. It tends to work best for nonsensitive operations that need significant computing power, such as high-frequency trading.

Private cloud

The private cloud is dedicated to a single organization and can be ideal for high-security operations, such as data storage and processing for retail banking.

Hybrid cloud

The hybrid cloud allows organizations to store sensitive data on a private cloud while leveraging the computing power of a public cloud for less sensitive operations.

	Public cloud	**Private** cloud	**Hybrid** cloud
Pros	✓ The public cloud provides access to vast, highly scalable computing resources in a cost-effective manner. It does not require users to purchase software or hardware, or to pay for resources beyond what's used.	✓ The private cloud offers a high degree of security and control. This platform is completely customizable.	✓ For many organizations, it combines the best aspects of public and private cloud models. The hybrid cloud provides both security and scalability.
Cons	✗ This platform is the least secure option due to its shared nature, which can create data security and privacy concerns. Compliance can be challenging due to shared resources and less control.	✗ The private cloud can be expensive to set up, especially for smaller organizations. It might not provide scalability without significant additional investment.	✗ Maintaining and integrating two different cloud environments can add complexity.

Choosing between types of services.

In addition to the three main cloud computing models, there are three main types of cloud computing services: infrastructure as a service (IaaS), platform as a service (PaaS), and software as a service (SaaS).

IaaS involves on-demand access to the physical and virtual back-end IT infrastructure needed to run applications and processes in the cloud. Typically, an organization would rent this infrastructure on a pay-as-you-go basis. IaaS is popular with startups and fast-growing companies because of its flexibility, scalability, and low up-front costs.

PaaS grants access to a ready-to-use, cloud-hosted platform that enables the development, testing, operation, and maintenance of cloud-based software. PaaS is often the choice for organizations that want to develop their own customized cloud apps without having to build the underlying infrastructure.

SaaS provides on-demand access to ready-to-use, cloud-hosted applications, usually on a subscription basis. The SaaS provider develops and maintains the software and any underlying infrastructure. SaaS often makes sense for organizations that don’t need complete customization of their cloud software and want to get up and running on the cloud fast.

These three types of offerings are not mutually exclusive or limited to particular cloud computing models, and many organizations use a mix of IaaS, PaaS, and SaaS. For larger organizations, it’s common to deploy all three for different purposes.

2 Steps to a successful cloud implementation

Every organization’s cloud transformation journey will look different, but there’s no need to proceed without a road map. Based on Crowe specialists’ experience with a wide range of clients, we’ve identified an overall methodology that can help your organization experience a smooth and strategic cloud rollout.

Step 1

Assess your organization’s current state

Before implementing a cloud solution, organizations need to understand their current IT infrastructure. This process involves:

→ **IT infrastructure audit.** Organizations should conduct a thorough audit of their current IT infrastructure, including hardware, software, data storage, and network capabilities. Then they should identify any outdated systems that need to be replaced or upgraded.

→ **Business process evaluation.** Evaluating current business processes and identifying areas where cloud solutions could improve efficiency and effectiveness is critical. Examples might include customer service, data analysis, or financial reporting.

→ **Regulatory compliance check.** Financial services organizations are subject to a variety of regulations, so they should review their regulatory compliance requirements. It’s crucial to confirm that any cloud solution that is implemented will support compliance.

Step 2

Identify the cloud solutions you want to use

Once organizations have assessed their current state, they can identify potential cloud solutions. This process involves:

→ **Vendor evaluation.** Research potential cloud vendors. Look at their reputation, the services they offer, their pricing models, and their security measures.

→ **Solution mapping.** Mapping out potential cloud solutions to identified needs can help organizations determine a best fit, which could include a combination of SaaS, PaaS, and IaaS solutions.

→ **Cost-benefit analysis.** Organizations should conduct a cost-benefit analysis of potential cloud solutions that considers upfront costs and potential long-term savings.

Step 3

Develop a cloud implementation strategy

Once potential solutions are identified, organizations can develop a cloud strategy. This step includes:

→ **Change management planning.** Organizations should develop a plan that details how they will manage the significant changes that come with cloud implementation.

→ **Strategy planning.** In addition to a change management plan, organizations should set a strategy plan that includes a timeline, budget, and identified milestones.

→ **Risk assessment.** Performing a risk assessment can help identify any potential risks associated with cloud implementation and develop strategies to mitigate them.

Step 4

Implement your cloud solution

With a strategy in place, organizations can then implement the cloud solution. This process typically includes:

→ **Technical implementation.** Implementation could involve migrating data, setting up new software, or configuring the network.

→ **Training.** Training might involve formal sessions for staff, one-on-one coaching, or self-guided learning resources.

→ **Monitoring and adjustment.** Organizations might need to troubleshoot technical issues, adjust strategy, or provide additional training based on the results of monitoring.

Step 5

Review and optimize the cloud solution

Implementing a cloud solution isn’t a one-time event. Rather, it’s an ongoing process that requires continual review and adjustment. This process involves:

→ **Performance reviews.** Organizations should determine how the cloud solution is affecting business processes, customer service, and bottom line.

→ **Security audit.** A security audit can help verify that your data is secure and that the organization is in compliance with all relevant regulations.

→ **Continual improvement.** Implementing an ongoing improvement process that might involve regular reviews, feedback sessions, and regular training can be helpful across the organization.

3 Add-ons that enhance security

Since financial services companies have a particularly high need for security, it's not always feasible to find a cloud service provider that satisfies all the security tenets that regulators and stakeholders require. So, organizations might want to consider the following add-ons:

Cloud access security broker

A cloud access security broker (CASB) is a software tool or service that sits between an organization's on-premises infrastructure and a cloud provider's infrastructure. A CASB acts as a gatekeeper, allowing the organization to extend the reach of its security policies beyond its own infrastructure.

What's the added value?

CASBs provide visibility into an organization's cloud applications and services use, data protection, and threat protection. They can help enforce security policies and comply with regulations, even when data resides in the cloud.

Configuration best practices to follow include:

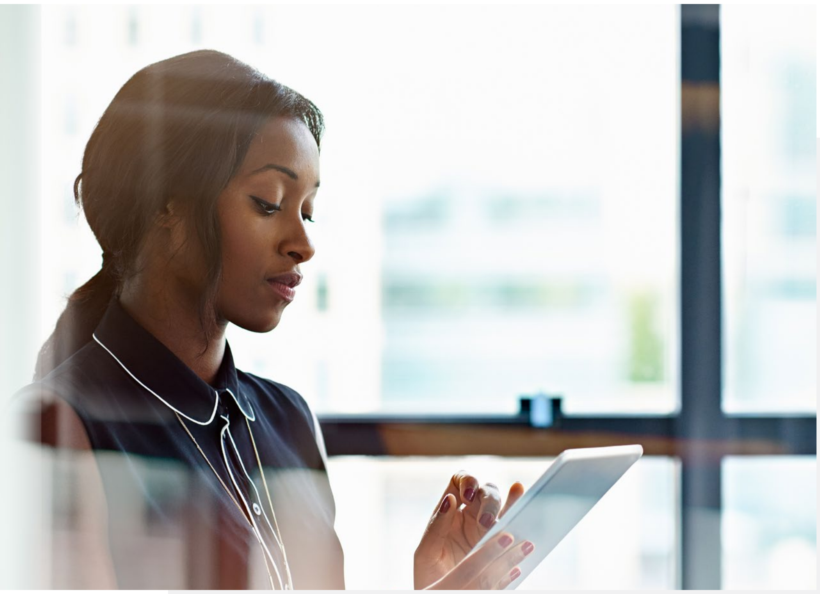
→ **Identifying sensitive data.** Before implementing a CASB, organizations should identify the types of data that are sensitive and where those data types reside in the cloud. This process will help in applying the appropriate security controls.

→ **Understanding user access.** Identifying who can use cloud services and what they can interact with is critical. The CASB can enforce access controls and monitor for any unusual or risky behavior.

→ **Encrypting data.** The CASB can encrypt sensitive data before it gets sent to the cloud. This can help protect data in transit and at rest.

Cloud security posture management

Cloud security posture management (CSPM) is a category of security tools that provides continuous compliance monitoring, visibility into cloud infrastructure security, and automated remediation of security incidents within cloud systems.



What's the added value?

CSPM tools can help an organization identify and remediate risks in real time, promoting compliance with security best practices and standards.

Configuration best practices to follow include:

- → **Continuous monitoring.** CSPM tools can continuously monitor cloud environments for any changes that could create security risks.
- → **Automated remediation.** CSPM tools can automatically fix security misconfigurations or alert the appropriate personnel when manual intervention is needed.
- → **Integration with CI/CD pipeline.** Integrating CSPM into the CI/CD (continuous intergration and continuous delivery) pipeline can help catch and fix security issues during the development and deployment process.

Cloud workload protection platforms

Cloud workload protection platforms (CWPPs) provide security technologies that are used to protect workloads in the cloud against threats. These platforms can protect any type of workload, including virtual machines, containers, and serverless workloads.

What's the added value?

CWPPs provide a unified security solution for all types of cloud workloads, which can reduce the complexity of managing multiple security tools.

Configuration best practices to follow include:

→ **Policy-based controls.** Organizations should implement policy-based controls that promote compliance with their security policies.

→ **Threat detection.** CWPPs can help detect and respond to known and unknown threats in real time.

→ **Integration with DevOps processes.** Integrating CWPPs into the software development and operations (DevOps) processes can help confirm that workloads are secure from the start of the development process.

Remember, the right configuration of these tools depends on specific cloud environment and security needs. Organizations should always follow the principle of least privilege, granting only necessary permissions, and regularly review and update security configurations as their cloud environment evolves.

4 Cloud post-implementation review

After the completion of the cloud implementation project, organizations should conduct a post-implementation review (PIR). This critical part of the cloud solution implementation process should evaluate whether project objectives were met, determine how effectively the project was run, glean lessons for future cloud and technology initiatives, and inquire whether the organization received the greatest possible benefit from the project and the resources involved.

Detailed steps of the post-implementation review process follow:

1 Planning the review.

This process involves identifying what will be reviewed, who will be involved in the review, and how the review should be conducted. The planning stage also includes setting the objectives for the review and defining the scope of the review.

2 Conducting the review.

With the review planned in full, the next step involves gathering data about the project and its outcomes. Data collection can occur through various means and channels, including interviews, surveys, and document reviews.

3 Analyzing the results.

Any data collected should undergo analysis to identify trends, patterns, and areas of concern. This stage compares the project's actual outcomes to expectations and evaluating the reasons for any gaps between the two.

4 Reporting the results.

The final report should include a summary of the findings, recommendations for improvements, and a plan for implementing these improvements for relevant stakeholders.

5 Implementing improvements.

Once the reporting team has delivered recommendations, organizations should build a plan for implementing the improvements, assign responsibility for the execution of the plan, and monitor the follow-through to confirm that the improvements are implemented correctly.

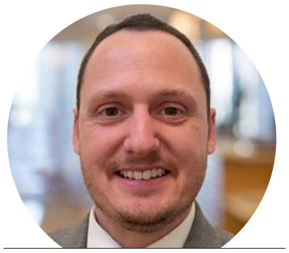
The goal of a PIR is not just to identify what went wrong but also to learn from the project and improve processes and strategies for future projects. With a thorough and curious approach to the review, organizations can hone a valuable tool for continual improvement.

A cloud journey can be a long and complex one. If you need help at any point, Crowe can be there.

A transition to cloud computing in the financial services industry demands meticulous planning, execution, and management.

But the journey can become a lot easier if you're guided by a team of financial services specialists with deep knowledge and expertise in cloud computing, technology, cybersecurity, regulatory compliance, and digital transformation. When you need help, call us. We can provide tailored, practical solutions that match your needs, goals, regulatory requirements, and resources.

Explore cybersecurity services



David R. McKnight
Principal
Financial Services Consulting
+1 630 575 4399
dave.mcknight@crowe.com

Timothy Tipton
Financial Services Consulting
+1 202 552 8093
timothy.tipton@crowe.com

Sign up to receive the latest cybersecurity insights on identifying threats, managing risk, and strengthening your organization's security posture.

Subscribe to Cybersecurity Watch

Crowe

Smart decisions. Lasting value.™

"Crowe" is the brand name under which the member firms of Crowe Global operate and provide professional services, and those firms together form the Crowe Global network of independent audit, tax, and consulting firms. "Crowe" may be used to refer to individual firms, to several such firms, or to all firms within the Crowe Global network. The Crowe Horwath Global Risk Consulting entities, Crowe Healthcare Risk Consulting LLC, and our affiliate in Grand Cayman are subsidiaries of Crowe LLP. Crowe LLP is an Indiana limited liability partnership and the U.S. member firm of Crowe Global. Services to clients are provided by the individual member firms of Crowe Global, but Crowe Global itself is a Swiss entity that does not provide services to clients. Each member firm is a separate legal entity responsible only for its own acts and omissions and not those of any other Crowe Global network firm or other party. Visit www.crowe.com/disclosure for more information about Crowe LLP, its subsidiaries, and Crowe Global.

The information in this document is not – and is not intended to be – audit, tax, accounting, advisory, risk, performance, consulting, business, financial, investment, legal, or other professional advice. Some firm services may not be available to attest clients. The information is general in nature, based on existing authorities, and is subject to change. The information is not a substitute for professional advice or services, and you should consult a qualified professional adviser before taking any action based on the information. Crowe is not responsible for any loss incurred by any person who relies on the information discussed in this document.

© 2023 Crowe LLP.