IDC ANALYZE THE FUTURE

IDC ANALYST BRIEF

Sponsored by: Oracle

As financial services organizations look to shift more workloads to public cloud, meeting security and compliance requirements is a key concern.

The Security and Compliance Benefits of IaaS for Financial Services

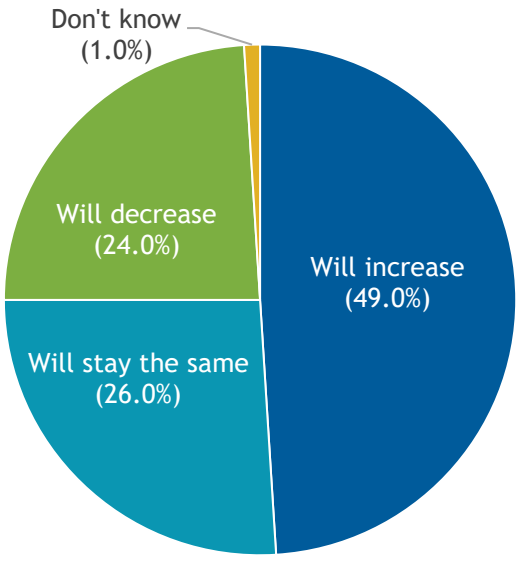
April 2021

Written by: Steven D'Alfonso, Research Director, IDC Financial Insights

FIGURE 1: ***2021 IaaS Investment Trends for Financial Services***

Spending plans for public cloud IaaS services

Q ***Compared to your organization's actual spending in 2020 (after COVID-related adjustments), how will your organization's planned spending (budget) on public cloud IaaS services change for 2021?***



n = 127

Source: IDC's Future Enterprise Resiliency and Spending Survey, February 2021

Financial Institution Security and Compliance Trends

Banking IT departments and CIOs are increasingly prioritizing cloud deployments as part of the overall digital transformation within the banking and financial service sector. There is an increasing demand for solutions that facilitate new and agile business models to boost employee productivity, enhance customer experiences, enable faster decision management capabilities through advanced analytics, and generally enhance efficiency across the organization. Cloud infrastructure is key to enabling these and many more technology initiatives.

Prior to 2020, the industry had been moving to public cloud as a viable deployment model as the percentage of IT investment in cloud (public and private) increased more than 53% between 2018 and 2020, outpacing investment in noncloud technology by sixfold. Response to the pandemic in 2020 served as a catalyst to accelerate investment in cloud. Cloud (public and private) spending is estimated to grow 10.9% over the next three years, nearly double the rate of overall IT spend for global banking (*IDC Perspective: Banking on Cloud: Results from the 2020 CloudPath Survey,* November 2020.) However, public cloud spending is expected to grow at 20.7% over the next five years, according to IDC's Worldwide 3rd Platform Spending Guide from October 2020.

Meeting security and compliance requirements in deploying cloud-based solutions is a key concern for financial services organizations as they look to shift more workloads to public cloud. Bank security compliance managers want to know how, from an infrastructure perspective, a cloud service provider (SP) will ensure that their compliance requirements are met. Additionally, bank security compliance managers want to understand how a cloud SP handles new or changing regulatory requirements.

Security for on-premises systems and applications has become complex. It is common for a bank's IT group to work with several security vendors, requiring integration and interoperability of numerous security tools. This often results in the use of multiple dashboards and workflows across many vendors. This security ecosystem makes adherence to security and compliance regulations quite complex.

Cloud IaaS offers financial institutions (FIs) the opportunity to alleviate the impact of their challenges, enhancing security and simplifying compliance.

IaaS Can Be a Path to Simplify Security and Compliance

Financial institutions make substantial investments in security and compliance tools to protect their assets and prevent compliance violations. However, the presence of these tools creates a complex environment that is challenging to manage. Complexity introduces operational risks to the information security ecosystem. Transitioning to an IaaS model can help alleviate many of the complexities involved with managing security and compliance requirements.

Under a shared responsibility model, an FI's IT group will gain the benefit of the cloud SP's expertise around applying infrastructure-related security controls. In addition, the cloud SP will assist with a portion of the security and compliance activities for which the FI is liable. As the end user, the FI will be responsible for configuring the cloud resources with guidance from the cloud SP. The exact breakout of responsibilities is somewhat dependent on the operating environment — that is, single tenant versus multitenant. The cloud SP will provide guidance related to best practices for security and configurability and should clearly delineate responsibilities for the shared security model. In addition, the cloud SP will provide security features and tools that the FI security team can leverage to ensure proper segmentation and encryption.

Many FIs have indicated to IDC that access to enhanced security features is a key driver for migration to the cloud. A cloud SP, generally, will have invested more in its people, processes, and technology than an individual financial institution. As a result, the FI benefits from the best-in-class technologies that the cloud SP can provide. Having one vendor that provides infrastructure security substantially simplifies security management by eliminating the need to coordinate the security tools related to multiple vendors in an on-premises structure. The combination of access to best-in-class technologies and simplified management of security controls enhances an FI's security posture.

From a compliance perspective, a cloud SP should provide added value by monitoring regulatory changes globally. An ongoing regulatory intelligence and change management capability will help FIs ensure security infrastructure compliance with supervising agencies and standard-setting organizations in the jurisdictions in which they operate.

Benefits of Adopting an IaaS Model

Using a cloud SP for IaaS has commonly known benefits such as improved performance and decreased capital expenditures as infrastructure becomes an operating expense, as well as increased scalability and flexibility. These benefits are important, but this document focuses on the security and compliance benefits related to IaaS.

Security Benefits

- Minimizing risk to business services provided to FI customers is paramount. IaaS will reduce the complexity associated with the multiple vendor solutions often used to manage an on-premises infrastructure, potentially eliminating vulnerabilities that can often creep into a complex ecosystem.
- The level of investment in security operations by a cloud SP is usually more than an individual FI can do, which means the FI benefits from an enhanced level of physical and network security. Cloud SPs design their infrastructure with security in mind to ensure that the data being protected and segmented is highly secure and free of malware.
- Security controls available through the cloud SP can help FIs optimize security configurations. Advanced features from cloud SPs will include automated security configuration assessments to identify issues, allowing an FI security administrator to identify and remediate misconfigurations quickly. In addition, cloud SPs will provide other automation services to apply machine learning to routine tasks, such as automated patching and automated database functions.
- Increased support for business continuity and disaster recovery will serve to shift the expense and responsibility of infrastructure resiliency to the cloud SP.

Compliance Benefits

- A cloud SP can provide continuous monitoring and assessment of regulatory requirements and apply controls that can help FIs meet their regulatory requirements. A global provider of IaaS to regulated entities, operating in multiple jurisdictions, can help FIs stay ahead of the regulatory curve.
- A cloud SP will often obtain industry security certifications such as SOC 2, PCI DSS, and ISO. Certifications will provide valuable assurance that key security requirements are being met. Further, independent third-party audits provide ongoing assurance. A cloud SP should also provide alignment documents to demonstrate how it meets regional or regulatory frameworks for which there are no certifications.
- Good security leads to good compliance outcomes. The security benefits that a cloud SP can provide, over and above what an individual FI can do on its own, will likely lead to consistent, reliable, simplified security compliance.

Considerations

While FIs have indicated that security is a key driver to transition workloads to the cloud, it should be noted that FIs also indicated to IDC that security is a significant concern of moving to the cloud. Using a cloud SP certainly introduces new risks for which an FI must adjust and plan to achieve a level of comfort for senior management, the board, and regulators. Not all cloud SPs are created equal; therefore, transparency on the part of the cloud SP and demonstrated experience working with other FIs and regulated entities should provide an adequate level of assurance. The good news, as IDC data indicates, is that there is a substantial shift to cloud within financial services, which indicates that regulators and board risk committees across the industry see the value and benefits of FIs moving to cloud.

Conclusion

Cloud IaaS offers numerous security and compliance advantages and benefits to financial institutions. Chief among those benefits are enhanced security and simplified compliance. Cloud SPs deliver best-in-class infrastructure security achieved through tremendous investments in people, processes, and technology. FIs can leverage these investments to improve security posture, automate security operations, and simplify security compliance activities.

Cloud IaaS offers numerous security and compliance advantages and benefits to financial institutions. Chief among those benefits are enhanced security and simplified compliance.

About the Analyst

Steven D'Alfonso, *Research Director, IDC Financial Insights*

Steven D'Alfonso is a Research Director with IDC Financial Insights responsible for compliance, fraud, and risk analytics strategies. His coverage area includes research on technology solutions aimed at solving key issues facing financial institutions around GRC regulations, financial crime, and risk management.

MESSAGE FROM THE SPONSOR

Oracle Cloud Infrastructure's build-in security and compliance solutions protect your most valuable data in the cloud. Oracle's approach leads with security first, built on our decades of experience securing data and applications. Oracle Cloud Infrastructure delivers a more secure cloud to our customers, building trust and protecting their data and:

- Strengthens security posture and reduces risk
- Reduces complexity and prevents human error with automated security tools
- Provides continuous protection with always-on encryption and continuous monitoring

Visit the Oracle Cloud Infrastructure ***security webpage*** to learn how Oracle Cloud Infrastructure is designed to protect our customers' data.

IDC Custom Solutions

The content in this paper was adapted from existing IDC research published on www.idc.com.

IDC Research, Inc.
140 Kendrick Street
Building B
Needham, MA 02494 USA
T 508.872.8200
F 508.935.4015
Twitter @IDC
idc-insights-community.com
www.idc.com