IDC

SPOTLIGHT

Sponsored by: Red Hat

Digital infrastructure forces IT executives to rethink how financial institutions should best approach digital transformation and to consider tools and platforms that help simplify what is becoming an increasingly complex environment.

Operationalizing Innovation in Financial Services Through Managing the Hybrid Environment

March 2022

Written by: Jerry Silva, Program Vice President, Global Retail Banking, IDC Financial Insights

Introduction

While 2020 proved a challenging year for almost all financial institutions worldwide, there were many organizations in the industry that benefited throughout the year from previous investments in digital transformation and the adoption of 3rd Platform technologies (cloud, big data/analytics, mobility, social). According to IDC's October 2021 *Future Enterprise Resiliency and Spending Survey,* those institutions experienced improvement in:

- Revenue (15% improvement)
- Decreased business risk (16% improvement)
- Improved time to market (19% improvement)
- Improved efficiency (19% improvement)
- Cost savings (21% improvement)
- Employee productivity (21% improvement)
- Profits (21% improvement)
- Innovation (21% improvement)
- Customer satisfaction (21% improvement)

These institutions are leading the shift from recovery to innovation through the investments made in digital transformation initiatives, particularly the investments in digital infrastructure. IDC defines digital infrastructure as the collection of technologies that span compute, storage, network, infrastructure software including virtualization and containers

AT A GLANCE

KEY STATS

According to IDC's October 2021 *Future Enterprise Resiliency and Spending Survey,* financial institutions that had previously invested in digital transformation benefitted from a 21% improvement in key categories during 2020, including:

- Customer satisfaction
- Innovation
- Profits
- Employee productivity
- Cost savings

WHAT'S IMPORTANT

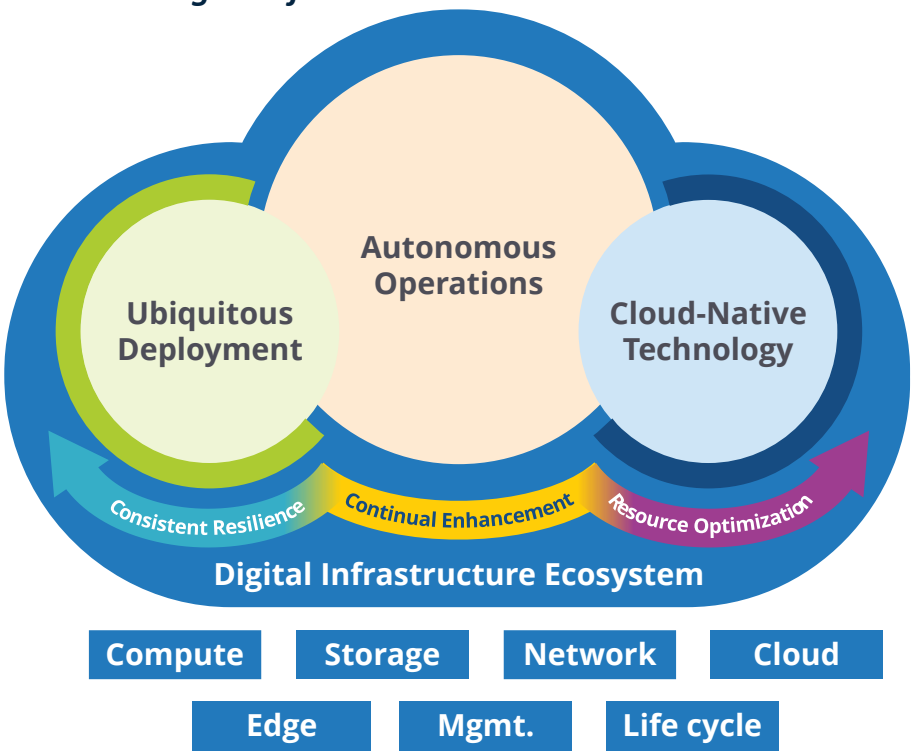
The ability to pivot from the challenges of 2020 and get back to the business of innovation has become a competitive advantage. But many financial institutions still struggle to move to the digital infrastructures necessary to make that shift.

KEY TAKEAWAYS

The need for partners and managed services to effectively leverage digital infrastructures has never been more pressing. Few institutions can manage the transformation to new development methodologies and deployment models across multiple cloud providers on their own.

and the automation, AI/ML analytics, and security software and cloud services needed to maintain and optimize both legacy and modern applications and data. Figure 1 depicts the digital infrastructure.

FIGURE 1: ***Digital Infrastructure***



Source: IDC, 2022

New Infrastructure Introduces New Challenges

These technologies hold the promise of enabling new operating platforms and modernizing legacy platforms that will drive financial services innovation going forward. However, the adoption of a digital infrastructure comes with challenges that are different than the way financial institutions have traditionally developed and delivered products and services:

- Lack of familiarity with some technologies (microservices, containers, etc.)
- Lack of skills in specific areas, like security
- New need for security and governance in hybrid cloud environments
- Need to reevaluate resiliency and scalability requirements in an expanded infrastructure
- Adopting new software development methodologies to leverage the new environment
- Changing the ways institutions manage the expanded digital infrastructure

These new requirements, in turn, translate into several undesirable outcomes if not addressed:

- Increased costs (inefficiencies)
- Slower time to market
- Focus on infrastructure rather than business needs
- Increased complexity managing cloud infrastructure
- Higher risks of downtime (decreases resiliency and scalability)
- Higher risk of security and compliance failure

What is needed to respond to this situation is a pivoting of the organization's IT structure and mindset to equip itself with the right people, tools, and partners to continue to accelerate the return to innovation. These new challenges of the industry's transformation are a given. But as IDC's 2021 *Worldwide Industry CloudPath Survey* (n = 300 financial institutions) shows, institutions chose "innovative offerings to support transformation" as their top criteria for choosing a cloud provider, signaling the importance of a digital infrastructure for the ability to innovate.

Cloud Is Key to Transformation

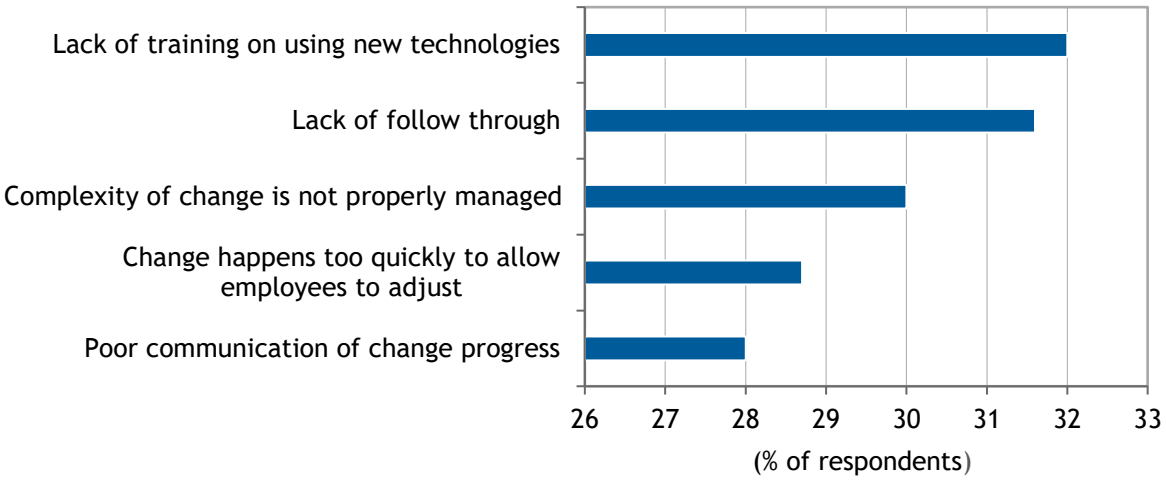
IDC defines hybrid cloud as the integration and orchestration between a private environment, including on premises and private cloud, and one or more public clouds. According to IDC's 2021 *Worldwide Industry CloudPath Survey* (n = 300 financial institutions), 35% of financial institutions globally currently operate in a hybrid cloud environment, with another 41% planning to do so into 2022. What is even more telling is that spend on cloud through 2025 is forecast to grow at 15.6% annually, while overall technology spend in global financial services is growing at half that rate, 7.5% annually through 2025. In fact, cloud investments accounted for 24% of total IT spend (hardware, software, and services) within the organization in 2021 but will increase to 31% of total IT spend by 2025 (source: IDC's Worldwide 3rd Platform Spending Guide, November 2021).

Clearly, the investment in cloud as a deployment model in financial services is accelerating tremendously, and this is true of related technologies and methodologies like APIs and microservices. These last technologies in particular have allowed institutions to make deployment decisions based more on business needs than technology requirements. In a sense, the new development mindset has become "build once, deploy anywhere." But institutions today continue to struggle to leverage the business opportunities in these new technologies.

In IDC's May 2021 *Worldwide Industry CloudPath Survey,* banks were asked to self-assess their ability to manage their cloud environments. Figure 2 shows that many institutions lack the tools and processes necessary to operationalize their hybrid environments and effectively innovate.

FIGURE 2: ***Institutions Struggle to Manage Hybrid Environments***

Q ***What is your organization finding most difficult when it comes to the change management involved in cloud adoption and usage?***



n = 100 global financial institutions

Source: IDC's Worldwide Industry CloudPath Survey, May 2021

What is clear from these responses is that many institutions worldwide still struggle to effectively take advantage of cloud, including development technologies like microservices and containers. In IDC's May 2020 *Worldwide Industry CloudPath Survey* (n = 373 financial institutions), 63–75% of institutions struggled with:

- Use of DevOps and/or continuous integration processes
- Ability to create/publish fully documented REST API with life-cycle capabilities
- Ability to accurately define costs and implement usage-based chargeback/billing mechanisms
- Mechanism for measuring the business value of the services provided
- Effective use of automation, self-service, and orchestration tools
- Development of custom applications using a microservices architecture
- Standardized ROI and business case tools to evaluate the costs and benefits of cloud resources
- Standard configuration and provisioning templates for cloud workloads and infrastructure
- Support of IoT and other real-time analytically based initiatives through an event-driven architecture
- Consistent service-level monitoring and reporting across private, hybrid, and public cloud applications and services

Likewise, security, always a major challenge for any financial institution, has come to the forefront of concerns as institutions focus on effective security strategies across the digital network. According to the ID Theft Resource Center, as of 2020, half of all attacks against financial institutions since 2005 have occurred over just the past five years. Ransomware attacks have also become a source of stress for financial institutions. In 2020, a major managed services organization (a firm that provides and operates technology platforms on behalf of financial institutions) fell victim to a ransomware attack, potentially affecting 9,000 individual institutions. Moving to a digital infrastructure that spans multiple cloud providers and datacenters makes the importance of orchestrating a robust security posture critical to the institution.

Managing hybrid cloud environments can include the following critical activities (aka cloud services):

- **Operational services** include the 24 x 7 management of cloud capabilities involving services such as asset management, performance management, capacity management, service catalog management, configuration management, event and fault management, identity and access management, security management, account management, and supplier management.
- **Strategic services** include such capabilities as strategy, assessment, migration, modernization, and implementation services.

The responses cited in the IDC surveys reveal the areas of cloud services with which IT executives have little familiarity. How does an institution develop business capabilities on one cloud services and migrate those efforts to a different one? What are the implications and effects of a disruption from a cloud-based workload on an on-premises application that depends on it? How can an institution minimize the impact of multiple development paradigms driven by a hybrid cloud infrastructure? Is every "link" in the chain of products and services across a hybrid environment secure?

To modernize and build the next-generation digital infrastructure, these (and others) are questions facing the next-generation technology executive that must be answered. These questions start with how the traditional "how-tos" of application development need to change and include the need to manage and orchestrate an infrastructure ecosystem of platforms, processes, partners, and people.

Benefits of Successful Development and Management in Hybrid Cloud Environments

The modernization of critical financial systems must leverage APIs, microservices, and containers to platform (or replatform) workloads to respond quicker to market needs and to gain efficiencies using cloud infrastructures. In addition, the flexibility and ability to deploy on the platform that makes the most sense for any specific workload, without undue impact on how that workload was developed, allows the institution to make better informed decisions about what to build, what to buy, what to consume, and in what form. If IT executives are successful in focusing more on the business priorities and standardizing the infrastructure to respond to those business needs, the institution will successfully pivot to accelerated innovation.

Efficiencies

The modernization of legacy workloads to modern languages and platforms, in and of itself, drives down the cost to build and maintain the applications. The modernization of the bank's core systems, more than any other systems, is being driven by this need to lower the costs associated with legacy languages (e.g., COBOL) and the need for in-house legacy platforms. Likewise, having the capacity to "develop once and deploy many" increases the efficiency to create business opportunities at lower costs.

Agility

Along with the efficiencies gained, the modernization to an API model leveraging microservices and containers provides an agility to not only deploy anywhere but update those applications in more of a real-time way than is possible in legacy instances. API libraries can also lead to low-code or no-code product development, where business analysts could compose innovative applications, using tested microservices, much faster than traditional methods. The use of containers is also key to resiliency and scalability, allowing the institution to respond in near real time to changing market conditions, including disruptive events.

Security and Compliance

It is hard to argue that as infrastructure complexity increases, so too does the opportunity for weaknesses and exposures in security and regulatory compliance. While the institution's goal is rightly to respond quickly to market needs and place customer satisfaction as a top priority, it cannot sacrifice either security or compliance to do so. But by creating a digital infrastructure using standard technologies, tools, and processes, it is actually easier to ensure security and compliance compared with ad hoc approaches to modernization and transformation being carried out in many institutions today.

Customer Satisfaction

In IDC's 2020 *Worldwide Industry CloudPath Survey,* when asked for the top benefit of moving to cloud, financial institutions responded with "improved customer experience." What is interesting here is that although the modernization of infrastructure is often, if not always, seen as a back-office initiative, the institutions are clearly signaling that the customer is directly impacted in a positive way, by the migration of applications and services to and the development of innovative services on cloud environments.

Leveraging Managed Cloud Services

Clearly, the benefits of moving to and managing successful cloud environments, particularly multicloud and hybrid cloud, will impel institutions to increase the adoption of cloud across the enterprise. But as cited previously, there are substantial challenges in doing so for most institutions expecting benefit from the digital infrastructure. Using a managed cloud services provider can reduce or eliminate many of the challenges and accelerate the business benefits of cloud by implementing operational best practices.

Lower Operational Costs

Managed cloud services can deliver cloud management at scale. Institutions don't have to acquire, train, and deploy specialized staff to operate in complex cloud environments. Typically, several distinct services are offered in a managed services package that an institution can pick from, depending on the internal support abilities.

More Agile Business Capabilities

Self-service capabilities are often a foundational aspect of a managed services environment. This places more control in the hands of the business leaders (while maintaining security, compliance, risk, etc.) so that the lines of business can direct the enterprise priorities as they wish, not as the technology dictates. In fact, in IDC's May 2021 *Worldwide Industry CloudPath Survey,* 44% of bank respondents listed "more direct control to business units" as an expected benefit from their cloud purchasing, usage, and strategy – the highest response of all other benefits listed.

IT Operations Efficiencies

The most obvious benefit from a managed services environment is the work done to "keep the lights on" and implement regular tasks to maintain and grow the infrastructure. From monitoring activities to upgrades ("evergreening") to applying patches and upgrades to maintaining secure and compliant environments, managed services providers use industry best practice and skilled resources to handle tasks like these. Institutions can eliminate the need to train staff and dedicate resources to what are usually mundane tasks.

Improved Resiliency and Reduced Risk

Saving the best for last, by using a managed services provider, the institution can again leverage industry best practice in the provider's abilities to monitor for, capture, and remediate disruptions as they occur. In conversations with banks, most admit that while they can usually identify and remediate simple disruptions, it can take hours to resolve problems in the infrastructure. When the disruptions are even larger, institutions often need the assistance of external partners to support the resolution of major disruptions. Managed services providers have established teams, processes, and practices that can support remediation faster than most institutions, reducing operational risk dramatically.

Considering Red Hat OpenShift Service on AWS

North Carolina–based Red Hat is a software and services provider founded in 1993, focused on open source technologies and whose offerings include Red Hat Linux, Red Hat OpenShift, its Kubernetes-based application platform, and Ansible, its automation solution, among other solutions. In 2019, Red Hat was acquired by IBM. The company now operates as an independent subsidiary.

Red Hat OpenShift Service on AWS (ROSA) is a cloud services offering, jointly operated and supported by Amazon Web Services (AWS) that enables financial institutions to develop containerized applications without the overhead and complexity of managing the cloud infrastructure itself. The service provides:

- Red Hat OpenShift, a platform that enables container-based application development and operation
- Availability on the AWS Management Console, with easy integration with other native AWS services
- Red Hat support and 24 x 7 site reliability engineering (SRE) that takes care of installing, maintaining, and upgrading the ROSA environment on behalf of the institution

The service ostensibly provides development resources at the institution to focus on the functional aspects of workloads without the need to manage the underlying platform. In addition, ROSA allows institutions to develop using one set of standards and deploy consistently across multiple cloud services platforms without the need to redevelop or migrate to accommodate different cloud providers, an important capability in the context of financial institutions adopting hybrid

cloud environments. The service follows the flexible, consumption-based model consistent with cloud services providers, avoiding the higher fixed costs of owning and managing the infrastructure internally.

Red Hat's goal for ROSA in financial services is to:

- Reduce costs through decreased operational overhead of resources needed in-house and for pay-as-you-go consumption
- Improve time to market for financial products and services
- Accelerate the use of cloud, microservices, and containers to improve agility and resiliency
- Shift development focus from infrastructure management to value-add business capabilities
- Increase developer productivity with integrated tools and services
- Address comprehensive security and compliance needs with industry-specific standards and regulations

ROSA is an additional deployment option of Red Hat OpenShift, giving organizations choice and flexibility of where they want to run OpenShift, either self-managed on premises or as a cloud service in the major public clouds. ROSA takes these capabilities further by providing the expertise of Red Hat site reliability engineers (SREs) to manage the platform for the institution, reducing the operational complexities of infrastructure management and ensuring a secure, reliable platform.

Challenges

ROSA seems to align with the needs and capabilities of institutions that don't have sufficient technology resources to manage and operate their development and infrastructure in a hybrid environment. This could arguably imply that larger institutions that have sizable technology resources might perceive competitive differentiation by managing their container environments themselves. Even then, some large institutions could decide they simply don't want to manage the environment themselves or may have hybrid environments where some deployments are more suitable for the ROSA offering. At an even smaller scale, thousands of institutions worldwide rely on a handful of managed services providers to supply all, or almost all, of their technology needs, including infrastructure, and who rely on those managed services providers to support their product needs. This leaves a relatively narrow band of institutions in whom the ROSA offering would resonate.

Likewise, the coupling together of existing platforms and services (AWS and Red Hat OpenShift) with support services does not, in itself, create a barrier to entry for other organizations to create similar offerings. Competitive services could emerge, making it more difficult for Red Hat to compete, even as an early provider.

Nonetheless, many financial institutions, regardless of size, will find ROSA compelling, especially in terms of adopting transformative technologies like cloud, microservices, and containers, in an effort to accelerate their return to innovation while lowering overhead and improving security and compliance.

Conclusion

The move to a digital infrastructure to support the benefits enjoyed by some institutions that have already invested in transformation is not without its challenges. Leveraging modern development tools on a digital infrastructure that spans from on-premises datacenters to multiple cloud deployments is becoming more complex, in turn risking potential weaknesses in time to market, costs, security, and compliance. As such, the digital infrastructure forces IT executives to rethink how the financial institution should best approach the transformation and consider tools and platforms that help simplify what is becoming an increasingly complex environment.

IDC believes that to succeed with digital transformation, the institutions and its IT leaders need to shift resources to focus more on business priorities and the management of partners and platforms rather than insisting on building infrastructure and development practices from the ground up. And the best way to do this is to pick partners and platforms that can support and simplify the responsibilities of the IT conductors and allow them to focus on the business of financial services.

About the Analyst

Jerry Silva, *Program Vice President, Global Retail Banking, IDC Financial Insights*

Jerry Silva is Vice President for IDC Financial Insights responsible for the global retail banking practice. Jerry's research focuses on technology trends and customer expectations and behaviors in retail banking worldwide. Jerry draws upon over 35 years' experience in the financial services industry to cover a variety of topics, from the back office to customer channels to governance in the technology shops at financial institutions.

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

This publication was produced by IDC Custom Solutions. The opinion, analysis, and research results presented herein are drawn from more detailed research and analysis independently conducted and published by IDC, unless specific vendor sponsorship is noted. IDC Custom Solutions makes IDC content available in a wide range of formats for distribution by various companies. A license to distribute IDC content does not imply endorsement of or opinion about the licensee.

External Publication of IDC Information and Data — Any IDC information that is to be used in advertising, press releases, or promotional materials requires prior written approval from the appropriate IDC Vice President or Country Manager. A draft of the proposed document should accompany any such request. IDC reserves the right to deny approval of external usage for any reason.

Copyright 2022 IDC. Reproduction without written permission is completely forbidden.