

WHITE PAPER

Delivering Organizational Impacts Based on EU Resiliency Regulations

Understanding the Path to Operational Resiliency and Compliance with Current EU Legislation with Capgemini and Red Hat

By Paul Nashawaty, Principal Analyst
Enterprise Strategy Group

August 2023

Contents

Executive Summary	3
Keeping Up with Ever-changing Regulations and Cloud Deployments	4
DORA at a Glance.....	5
Preparing for DORA.....	6
DORA Challenges for Firms Heavily Relying on Non-EU CSPs	6
Creating a Cloud Strategy for Compliance.....	7
Cloud Sovereignty Layer: What It Is and Why It Is Required	7
Research Shows Most Applications on Multiple Clouds.....	8
Getting Started with a Best Practice Methodology.....	9
Day 1: Assess and Plan the Journey	9
Day 2: Set Up People, Processes, and Technology	9
Day 3: Deliver and Operate First-mover Applications.....	10
Day 4: Build Capability and Scale Containerization Across the Organization.....	10
When Cloud-native Makes Sense	11
Case Study in Action: Creating a Strategy for Cloud Mobility	11
Conclusion	11

Executive Summary

New European Union (EU) regulations are in the works to streamline the third-party risk management process across financial institutions. The Digital Operational Resilience Act (DORA) is the EU's attempt to establish a detailed and comprehensive framework to harmonize various regulatory initiatives and create an objective Information and Communication Technology (ICT) risk management standard for Europe. Designed to improve operational resiliency of the financial services sector, DORA helps ensure EU-based financial services organizations mitigate risks arising from increasing reliance on ICT systems and third parties for critical operations. Although DORA has gained the most traction, similar pieces of regulation are currently under consideration around the globe.

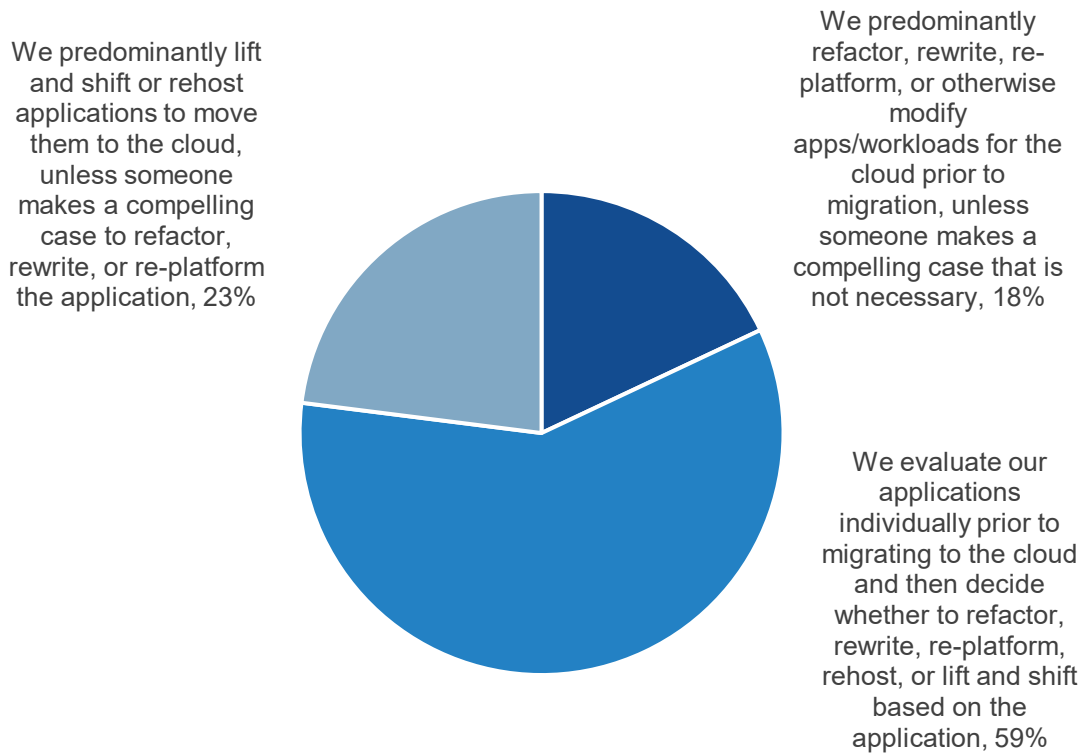
DORA includes provisions governing the management of risks associated with financial entities' outsourcing to technology service providers (TSPs), including cloud service providers, and it mandates direct oversight of "critical" TSPs. This proposed policy is designed to ensure EU-based financial services organizations using a single cloud service provider (CSP) have a documented strategy around portability—that is, the ability to quickly and seamlessly shift critical data and workloads to and from their current CSP to another, such as a local cloud provider, colocation, or another hyperscale provider. The policy may also require proof of the ability to exit the CSP relationship if circumstances warrant it. In addition, financial services firms need documentation proving this portability capability has been tested. The key benefit coming from this legislation is that it enables more robust operational resilience in the finance ecosystem by empowering organizations with the ability to build, assure, and review their technological operational integrity. It means that when an organization has a security threat or unexpected provider downtime or lack of access to the application, the organization has the means to respond, recover, learn, and adapt. Another benefit is that it can increase cloud sovereignty and prevent overreliance on foreign CSPs, such as Google, AWS, and Microsoft Azure. Although these new regulatory requirements offer organizational and consumer benefits by ensuring less reliance on a single provider, they impact how financial services companies work with CSPs and other third parties and require rethinking of existing cloud strategies.

Although DORA is targeted to the financial services sector, this regulation will likely be adopted more broadly across industries, countries, and continents. Capgemini, in partnership with Red Hat, has developed a streamlined containerization service methodology to lead global organizations through the process. The approach establishes a multi-cloud strategy, designs and delivers an implementation built on "first-mover" applications, and provides skilled people to deploy the right Red Hat technologies. According to research from TechTarget's Enterprise Strategy Group, 77% of organizations are either evaluating their applications prior to migrating them to the cloud or are fully committed to refactoring their applications when going to the cloud (see Figure 1).¹

¹ Source: Enterprise Strategy Group Complete Survey Results, [Distributed Cloud Series: Application Infrastructure Modernization Trends](#), March 2022.

Figure 1. Organizations’ Approaches Prior to Migrating to the Cloud

When moving applications/workloads to the cloud, which of the following best aligns with your organization’s approach (i.e., whether you refactor, rewrite, or otherwise modify the application) prior to migrating to the cloud? (Percent of respondents, N=36)



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

In addition, Capgemini helps develop a dynamic roadmap for the organization to follow. In this paper, we explore what it means for financial services firms to leverage DORA and how it stands as a unifying directive aimed at guaranteeing that financial service entities functioning within the EU adhere to proper third-party risk management procedures that are duly reviewed, documented, and attested. A notable ramification of DORA pertains to its potential influence on an institution's choice regarding the migration of vital applications and functions to a singular or multiple cloud service providers (CSPs), potentially neglecting essential portability attributes.

Keeping Up with Ever-changing Regulations and Cloud Deployments

Most financial services organizations started their journey to the cloud many years ago, with some being early adopters of a cloud-first strategy. Now, with upcoming regulatory changes in the EU such as DORA, all EU-based financial services organizations are being forced to rethink how they use clouds, which clouds they use, and for what services. DORA, the legislative proposal from the European Commission currently in draft, requires financial institutions to have safeguards in place to mitigate risks that could bring down significant infrastructure, such as an entire region of a global CSP. An integral component of the enacted legislation, effective as of January 2023 and mandating likely compliance within the ensuing 24 months, entails that financial service entities establish and

document a structured strategy. This strategy should showcase their capacity to efficiently transfer their cloud-based data (workloads) among various cloud service providers and/or revert to on-premises data centers swiftly. Furthermore, they are required to furnish evidence of testing this portability proficiency as a viable method. It's important to note that DORA does not impose an obligation for portability. The scope of this regulation encompasses financial services firms employing a single non-EU cloud service provider, like AWS, Azure, or Google Cloud, regardless of the CSP's location—whether within the EU or outside it. The comprehensive range of relevant parties and considerations is elaborated in the regulation.

DORA at a Glance

While DORA became law in 2022, it can be used as a proxy for other regulations that are already in place or are being considered around the world. The DORA requirements across its five pillars include:²

1. ICT risk management.
 - Protect and prevent ICT risks by implementing adequate technical and organizational mitigation measures.
2. ICT-related incidents management, classification, and reporting.
 - Identify, classify, and document all ICT-related business functions, information assets supporting these functions, and all sources of risk.
 - Perform an ICT risk assessment at least annually.
3. Digital operational resilience testing.
 - Detect single points of failure and unusual activities through regular testing.
 - Respond to disruption and recover from incidents by implementing a dedicated and comprehensive ICT business continuity plan and an ICT disaster recovery plan, respectively, with both maintained and tested regularly.
4. ICT third-party risk management.
 - Strengthen the outsourcing rules governing the indirect oversight of ICT third-party providers.
 - Enable a direct oversight of the activities of ICT third-party providers when they provide their services to financial firms.
 - Incentivize the exchange of threat intelligence in the financial sector.
5. Information and intelligence sharing.
 - Learn, evolve, and communicate by analyzing the root causes of incidents and the effectiveness of the protection and detection measures in place.
 - Ensure communication plans, enabling a responsible disclosure of ICT-related incidents or major vulnerabilities to clients, counterparts, and the public.

Financial Services and DORA Pillars

This paper explores aspects of the second and fourth pillars and the impact on the financial services industry, such as payment institutions, investment firms, credit rating agencies, crypto-asset service providers, crowdfunding service providers, fintech, trading venues, financial system providers, and credit institutions.

² Source: [Commission Staff Working Document: Executive Summary of the Impact Assessment Accompanying the Document, Proposal for a Regulation of the European Parliament and of the Council on digital operational resilience for the financial sector and amending Regulations \(EC\) No 1060/2009, \(EU\) No 648/2012, \(EU\) No 600/2014 and \(EU\) No 909/2014.](#)

Preparing for DORA

Although companies will not be mandated to use a local cloud provider, DORA aims to limit dependence on a single CSP. And this will require extreme portability—that is, the ability for infrastructure to quickly move a portion of critical workloads and data back and forth between clouds and on-premises environments.

There are three key considerations to achieving operational resiliency and less dependence on a single CSP:

- **Mandatory option:** The essence lies in having a contingency plan, where portability could offer a solution, yet the regulations themselves won't dictate the specific remedy for enterprises, including the implementation of DORA requirements and the development of a cloud sovereignty layer on top of the non-EU CSP.
- **Option A:** DORA requirements encompass facilitating the utilization of EU-based CSPs for essential workloads, particularly in instances where internal hosting is unfeasible. These regulations emphasize the importance of ensuring seamless and compliant transitions to EU-based CSPs to uphold operational continuity and regulatory alignment.
- **Option B:** This involves moving workloads or data back to in-house data centers. Depending on the service, it may be easier to move the application in-house than to make all the coding changes to move it to a different CSP. While the long-term strategy of moving everything back to a data center is costly, if something goes wrong, the fastest way to continue services (which is what a regulator will care about—customer impact) may be in-house.

DORA Challenges for Firms Heavily Relying on Non-EU CSPs

DORA underscores the necessity for organizations to reassess their strategies and explore avenues to alleviate the risks tied to third-party outsourcing. A potential approach for risk mitigation involves embracing an infrastructure conducive to a hybrid cloud strategy, incorporating portability as a key element. By doing so, firms can proactively enhance their operational resilience and regulatory compliance.

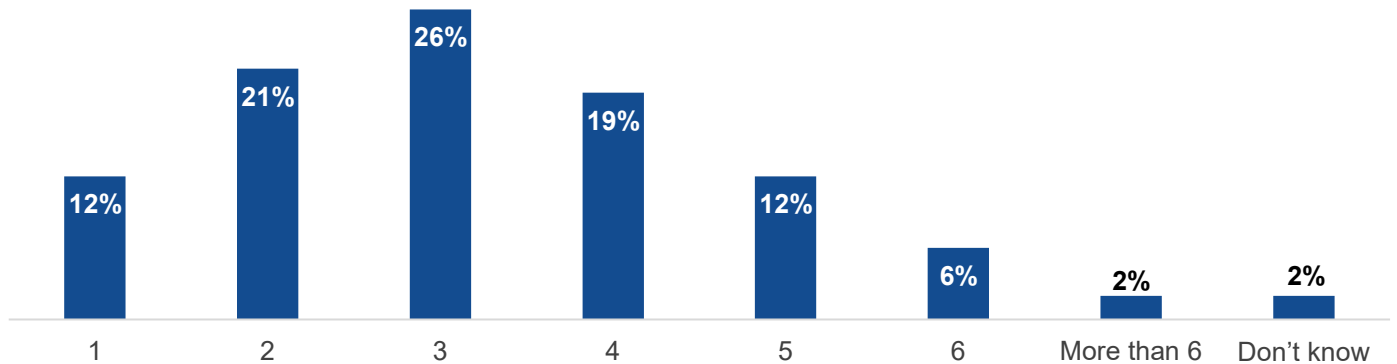
Enterprise Strategy Group research shows that 86% of organizations are already using multiple cloud service providers as part of their estate (see Figure 2).³

Occasionally, this occurs inadvertently, where the cloud hosting of a SaaS offering goes unnoticed, while in other cases, it's a deliberate choice. The emergence of regulations like DORA, along with forthcoming ones, will compel organizations to adopt more deliberate approaches to their technology stack and its alignment with their multi-cloud strategy.

³ Source: Enterprise Strategy Group Research Report, [Application Infrastructure Modernization Trends Across Distributed Cloud Environments](#), March 2022.

Figure 2. Nearly 9 in 10 Organizations Use More Than One Cloud Service Provider

**Approximately how many unique public cloud infrastructure service providers (IaaS and/or PaaS) does your organization currently use?
(Percent of respondents, N=321)**



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

However, achieving this level of portability can be especially challenging when trying to move from a singular U.S.-owned cloud service provider to an EU-based cloud service provider because of the higher-level services, such as database-as-a-service, within the U.S.-owned cloud. In addition, when the infrastructure foundation is based on a proprietary toolset, portability becomes even more problematic.

Creating a Cloud Strategy for Compliance

The names of the game for creating compliance are *portability* and *proof*. When moving the data back on premises is not an option, financial services firms using a single CSP will need to:

- Incorporate a "cloud layer" into DORA stipulations, operating atop the chosen CSP, or collaborate with a CSP that already employs such technology. This step aims to enhance provider independence, data security, and the ability to revert, typically encompassing foundational cloud services like security, compliance, and monitoring, as well as CSP-agnostic orchestration, configuration, operations, FinOps, security, and compliance solutions layered over CSP services.
- Employ supplementary CSPs, potentially incorporating a prominent industry player alongside regional EU-based CSPs, to address particular, less extensive workloads demanding tailored data compliance measures due to the nature of stored and utilized data—especially sensitive proprietary data—particularly when on-premises alternatives are unavailable. It's important to note that while this isn't mandated by DORA, it stands as a robust recommendation.
- Foresee where the evident value of OpenShift translates into efficiency. Constructing applications on a versatile platform like OpenShift not only signifies resilience but also avoids the time-consuming consequences of lacking advanced planning. While transitioning back on premises is an option, it demands meticulous planning and might not be the most time- or cost-efficient choice, in addition to potentially inhibiting innovation compared to a cloud-based strategy.

Cloud Sovereignty Layer: What It Is and Why It Is Required

Sovereign clouds are architected and built to deliver security and data access that meets strict requirements of regulated industries and local jurisdiction laws on data privacy, access, and control. They protect and unlock the

value of critical data for private and public sector organizations. Creating a sovereign cloud involves building several sublayers and shared responsibilities between the service provider and the organization.

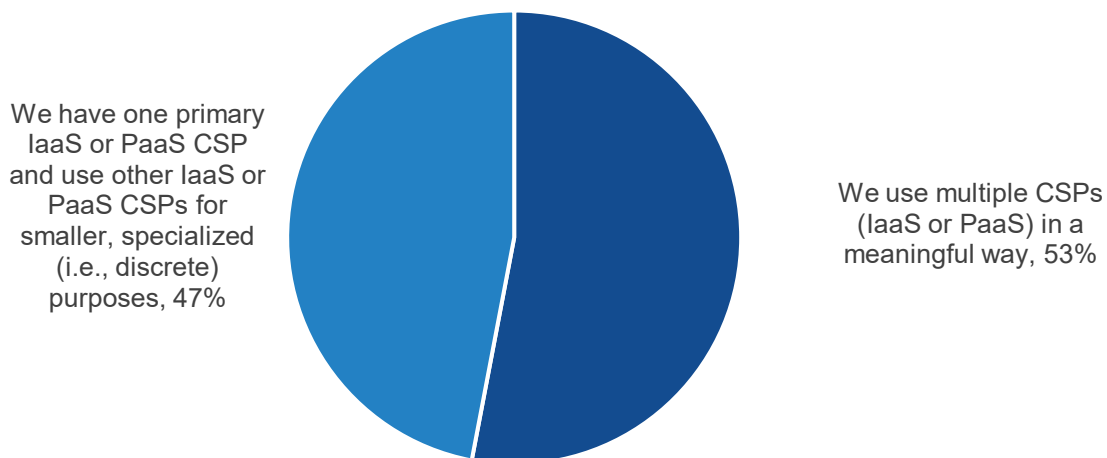
When built on an open platform with open technologies, the cloud sovereignty layer enables the required operational resiliency and the portability of applications and workloads, data security, and data access for easy migration between clouds.

Research Shows Most Applications on Multiple Clouds

Enterprise Strategy Group research shows that 63% of organizations have applications that are on multiple clouds, which can include the entire application in multiple cloud service providers or different components of the same application that leverage specific cloud service provider capabilities (see Figure 3).⁴

Figure 3. Applications Live in More Than One Cloud Today

You mentioned you consume public cloud infrastructure services from at least 2 unique CSPs. How would you describe this usage? (Percent of respondents, N=279)



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Demonstrating and testing the portability of applications in the infrastructure will be critical to meeting DORA regulations to ensure operational resiliency. DORA assesses organizations on which applications represent a risk to achieving operational resiliency, and, as mentioned, will likely focus on those that run on a single third-party cloud service provider.

Applications hosted on a flexible, open cloud platform offer the ability to build, deploy, and operate those applications using multiple CSPs. As a result, an open platform provides the portability—the agility—required as part of the DORA mandate. Third-party management will be viewed with more scrutiny, which is why organizations need to document their strategy and test their plan to demonstrate that the required level of operational resiliency is met.

⁴ Source: Enterprise Strategy Group Complete Survey Results, [Distributed Cloud Series: Application Infrastructure Modernization Trends](#), March 2022.

Getting Started with a Best Practice Methodology

Ideally, organizations need to look at how they are building the applications from the start of development. If applications are made “resilient” from the outset—meaning they are built on open platforms (like Red Hat)—it is easier to demonstrate portability and prove that the applications can be moved and that the data is easily accessible, which satisfies compliance and mitigates risk.

If it is not possible to have a portability plan between clouds, the organization must be able to demonstrate it has an “escape plan” from that cloud service provider. This requires “reversibility,” which is the ability to securely migrate applications and data from a CSP to another CSP or back on premises.

The cloud journey to DORA compliance through the use of application containerization can be complex. Let’s take a look at how Capgemini, partnering with Red Hat technologies, engages with financial services firms to help them manage the entire process, be compliant, and gain the operational resiliency required for greater cloud sovereignty and enhanced disaster recovery.

This plan is based on a foundation of service blocks, combined with Red Hat OpenShift Container Platform, and embedded into the cloud journey where appropriate. Those service blocks are the building blocks to sustainable multi-cloud success. Capgemini advises and assesses the current environment, provides patterns to the organization for Red Hat OpenShift Engineering and Operations, develops and executes a workload migration and modernization plan, augments and builds capability for cloud-native build and operations skills, provides patterns and people for site reliability engineering, and helps the organization with talent building throughout.

Day 1: Assess and Plan the Journey

Working with financial services organizations, Capgemini helps assess and plan the journey to cloud development and deployment. This can include producing a hybrid or multi-cloud model based on feedback from the following questions:

- Does the application present a significant risk to customers if it becomes inaccessible? Is it business-critical?
- Are the apps fine as is or do they need to become cloud-enabled and ready for today and tomorrow?
- What are the internal SLOs for the applications in the cloud, and what are the SLAs to the end consumer of the data? How do those SLAs translate to meet an organization’s regulatory obligations?
- Can the organization demonstrate that portability is built into the model, that it is tested, and that the data is accessible and secure?
- How will an organization move workloads and the associated data? What is its disaster recovery plan that covers and enables multi-cloud?

Day 2: Set Up People, Processes, and Technology

The next step is to set up the people, processes, and technology. Using Capgemini cloud strategy expertise and leveraging the Red Hat technology stack, begin building an architecture blueprint. This blueprint becomes a part of an organization’s cloud strategy documentation and proof to regulators.

An organization should start by building the cloud sovereignty layer, which consists of:

- Cloud service management and integration (DevOps enablement layer) - Red Hat Advanced Cluster Management for Kubernetes.
- Cloud orchestration and configuration - Red Hat OpenShift Container Platform; Red Hat Ansible Automation Platform.

- Cloud operations - Red Hat OpenStack Platform.
- FinOps (cost management) - Red Hat OpenShift Container Platform.
- Security and compliance - Red Hat Advanced Cluster Security (ACS) for Kubernetes.
- Platform-as-a-service (PaaS) - To determine where and what higher-level services are required.
- EU and non-EU CSP strategy - To build a strategy that takes into account current and future CSP locality and IaaS capabilities.
- Cloud competence center, global product teams, and migration factory - Red Hat 3Scale API Management; Red Hat Fuse Online.

Under the cloud sovereignty layer, organizations can set up a cloud service management and integration layer (i.e., a DevOps enablement layer, such as Red Hat Advanced Cluster Management for Kubernetes).

Next, they should set up local cloud competence centers (within BUs/countries) responsible for local cloud service management, onboarding and training, local automation, and integration into the local application landscape using technologies like Red Hat 3Scale API Management and Red Hat Fuse Online.

Then, they should set up the cloud orchestration and configuration layer (for example, from Red Hat OpenShift Container Platform and Red Hat Ansible Automation Platform).

There will be a shared responsibility between local cloud competence centers and global product teams around cloud orchestration and configuration management, cloud operations (e.g., platform operations), cost management, and cloud security and compliance.

In addition, the underlying infrastructure needs to be a PaaS, IaaS, or XaaS layer. It is important to set up global product teams and cloud broker units for the development of PaaS, IaaS, and XaaS foundation layers on top of CSP offerings, such as security, data privacy ruleset, bring your own encryption key (BYOK), monitoring, logging, security operations center (SOC), and IT service continuity management (ITSCM)/IPC.

Day 3: Deliver and Operate First-mover Applications

The third step in this methodology leverages the first two steps to identify first-mover applications. Organizations need to focus on working with their development “squads” to determine their readiness for applications, not only to be designed right for the cloud environment but also to be ready for management in the cloud. This means that all of the CI/CD pipelines, automation playbooks, and ongoing observability are built for and capable of being managed in that way.

Day 4: Build Capability and Scale Containerization Across the Organization

The fourth step focuses on ongoing operations, building of the internal talent capabilities of the organization, and scaling of the containerization platform methodology. During Day 4, organizations:

- Focus on building internal organizational capabilities, with the goal of operating the cloud strategy as the blueprint.
- Should expect a transfer of knowledge and run books, enabling onboarding of future talent and ensuring that institutional knowledge is documented.
- Augment talent until it is attained and trained on operating procedures.

When Cloud-native Makes Sense

Red Hat partners with global systems integrators (GSIs) like CapGemini around the world to deliver intelligent, secure cloud solutions. Using its Red Hat OpenShift Container Platform and other technologies, Red Hat enables DORA compliance and helps companies to achieve:

- Greater cloud adoption and all the inherent benefits, such as speed of innovation and cost optimization on multi-cloud, hybrid cloud, secure cloud, edge computing, cloud transformation, and data center exit.
- IT transformation, including technical debt reduction, FinOps, sustainable IT, and IT modernization.
- Business innovation, including microservices, digital twins, data science/machine learning, DevSecOps, and cloud-native applications.
- Intelligent industry, including IoT, data analytics and insight, real-world modeling, rapid integration of products/services, and rapid scaling.

Case Study in Action: Creating a Strategy for Cloud Mobility

The following case study details a real-world reference architecture blueprint created for an open, sovereign cloud using Red Hat. The organization engaged with Capgemini and Red Hat to ensure that they would be positioned to take advantage of the cloud and able to guarantee cloud portability.

Who: A large, global technology services provider.

Challenge: The organization had a few delayed or failed cloud journeys in the past. The organization had to design and deliver a large-scale reference proof of concept (PoC), designed to help solve its previous issues with the cloud, efficiently and at lower risk.

Solution: The organization had to build an enterprise-ready, open, hybrid/multi-cloud environment that allowed demonstration or testing of specific solutions from preconfigured use cases or to-be-developed PoCs that could be created by leveraging combined knowledge.

Results:

- The organization moved over 500 apps to Red Hat OpenShift on private cloud and public cloud throughout Switzerland and within Azure.
- The organization created a four-year plan, launching a subset of 600 applications in Switzerland and Azure.
- 120 apps were migrated to Azure Red Hat OpenShift.

Conclusion

The cloud journey is not a new story, but regulations like DORA—and others similar to it that are emerging around the globe—force all companies, not just financial services firms, to add a new chapter to their cloud playbooks. DORA requires enterprises to rethink their cloud strategies to achieve enhanced portability and new benefits, like the highest digital operational resilience and security standards possible, all while focusing on accelerated innovation and implementing technologies under a secure and harmonized multi-cloud framework.

At a high level, DORA-related activities require organizations to reexamine their current cloud strategy and:

- Conduct a maturity assessment against the requirements and define a mitigation plan.
- Start collecting and documenting resilience information for all third-party cloud service providers.
- Define and execute a test for a potential scenario of an ICT outage.

It's important to keep in mind all the potential benefits from DORA regulations that can help organizations, including:

- Addressing ICT security, outage, and disaster risks more comprehensively.
- Enabling easier access to information on ICT-related incidents.
- Ensuring that organizations understand and document the effectiveness of their resilience measures and identify ICT vulnerabilities.
- Achieving cloud strategies that take advantage of outsourcing rules governing the indirect oversight of ICT third-party providers.
- Directing oversight of the activities of ICT third-party providers that provide services to financial firms.
- Incentivizing organizations in the financial services sectors to exchange information on threat intelligence.

Those organizations planning to adhere to DORA regulations need to be thoughtful about the steps for their cloud strategies. They have to involve intentional, not accidental, adoption of multi-cloud. Some companies may choose to bring applications, data, and workloads back to on-premises data centers, but for many, the hit in cost and innovation capabilities will make this an unattractive option. Organizations need to consider how they balance their apps, data, and workloads between their current CSP and another CSP, possibly a local provider. And they must have this strategy documented and tested.

It's worthwhile to consider leveraging the expertise of a company like Capgemini, which is using open platform technologies like Red Hat's to ensure organizations are resilient, secure, tested, documented, and ready for the next set of regulations.

©TechTarget, Inc. or its subsidiaries. All rights reserved. TechTarget, and the TechTarget logo, are trademarks or registered trademarks of TechTarget, Inc. and are registered in jurisdictions worldwide. Other product and service names and logos, including for BrightTALK, Xtelligent, and the Enterprise Strategy Group might be trademarks of TechTarget or its subsidiaries. All other trademarks, logos and brand names are the property of their respective owners.


Information contained in this publication has been obtained by sources TechTarget considers to be reliable but is not warranted by TechTarget. This publication may contain opinions of TechTarget, which are subject to change. This publication may include forecasts, projections, and other predictive statements that represent TechTarget's assumptions and expectations in light of currently available information. These forecasts are based on industry trends and involve variables and uncertainties. Consequently, TechTarget makes no warranty as to the accuracy of specific forecasts, projections or predictive statements contained herein.

Any reproduction or redistribution of this publication, in whole or in part, whether in hard-copy format, electronically, or otherwise to persons not authorized to receive it, without the express consent of TechTarget, is in violation of U.S. copyright law and will be subject to an action for civil damages and, if applicable, criminal prosecution. Should you have any questions, please contact Client Relations at cr@esg-global.com.

About Enterprise Strategy Group

TechTarget's Enterprise Strategy Group provides focused and actionable market intelligence, demand-side research, analyst advisory services, GTM strategy guidance, solution validations, and custom content supporting enterprise technology buying and selling.

 contact@esg-global.com

 www.esg-global.com