Enterprise Strategy Group by TechTarget

DELIVERING ORGANIZATIONAL IMPACTS BASED ON EU RESILIENCY REGULATIONS

Capgemini and Red Hat are focused on helping organizations understand the path to operational resiliency and compliance to current EU Digital Operational Resilience Act (DORA) legislation. Although DORA has gained the most traction, similar pieces of regulation are currently under consideration around the globe. Designed to improve the operational resiliency of the financial services sector, DORA helps ensure EU-based financial services organizations mitigate risks arising from increasing reliance on information and communications technology (ICT) systems and third parties for critical operations.

This Enterprise Strategy Group Infographic was commissioned by Red Hat and is distributed under license from TechTarget, Inc.

Management of risks associated with financial entities' outsourcing to cloud and technology service providers mandates direct oversight

Before DORA, financial institutions, 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, managed the main categories of operational risk mainly with the allocation of capital, but they did not manage all components of operational resilience.

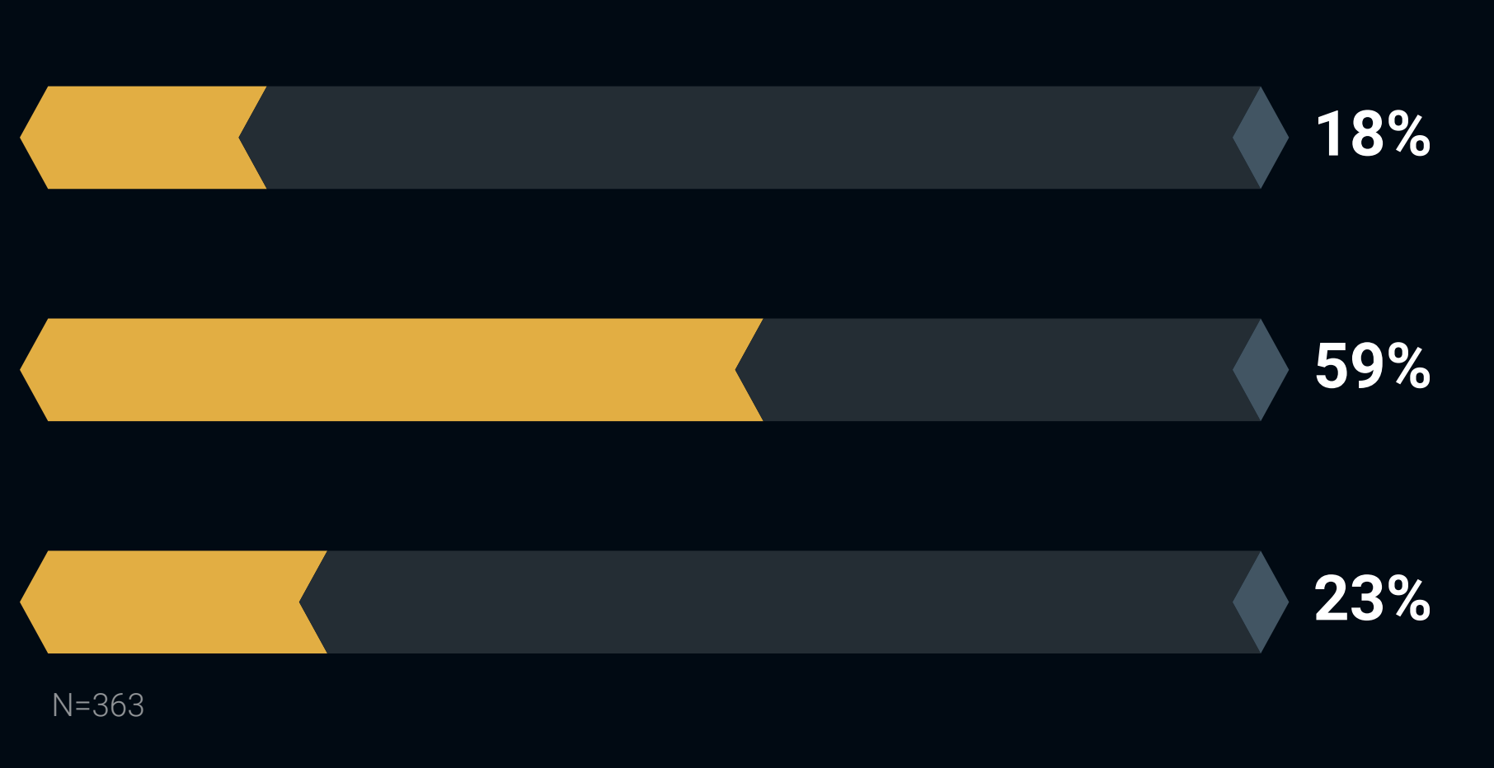
DORA stands as a unifying directive aimed at guaranteeing that financial service entities functioning within the EU have reviewed, documented, and attested to proper third-party risk management procedures. A notable ramification of DORA pertains to its potential influence on an institution's choice regarding the migration of vital applications and functions to a single or multiple cloud service providers (CSPs) without considering necessary portability features.

Organizations' Approaches Prior to Migrating to the Cloud

We predominantly refactor, rewrite, re-platform, or otherwise modify apps/workloads for the cloud prior to migration, unless someone makes a compelling case that is not necessary

We evaluate our applications individually prior to migrating to the cloud and then decide whether to refactor, rewrite, re-platform, rehost, or lift and shift based on the application

We predominantly lift and shift or rehost applications to move them to the cloud, unless someone makes a compelling case to refactor, rewrite, or re-platform the application



N=363

Components of Application Migration

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.

An integral component of the enacted legislation, effective January 2023, with compliance likely being mandated within the ensuing 24 months, entails that financial service entities establish and document a structured strategy. This strategy should showcase the entities' capacity to efficiently transfer their cloud-based data (workloads) among various CSPs 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 CSP, 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 upon in the regulation.

DORA at a Glance

DORA serves not only as a standalone regulation but also as a benchmark for other existing and potential regulations worldwide. The comprehensive framework of DORA's requirements, spanning its five fundamental pillars, establishes a harmonized approach toward enhancing financial services' resilience and risk management practices. This harmonizing regulation sets a precedent for global efforts in fortifying the industry's operational robustness.

DORA focuses less on the specifics and more on ensuring that firms establish contingency plans for outsourced critical systems, thus ensuring customer service continuity, with clear articulation, regular war-gaming, and testing. It also aims to harmonize regulations like MiFID II, PSD2, and GDPR, streamlining their compliance requirements alongside DORA's framework.

Red Hat believes that **DORA underlines the essential requirement for a robust infrastructure**, emphasizing the potential of a hybrid cloud approach as a means of achieving resilience. This approach enables the adoption of "build once, deploy anywhere" strategy, which can contribute significantly to bolstering an organization's overall resiliency.

In the realm of ICT risk management, there are several crucial aspects to address. This involves implementing effective technical and organizational mitigation measures to both safeguard against and preempt ICT-related risks. An integral part of this process is the comprehensive management of ICT-related incidents. This encompasses the identification, classification, and meticulous documentation of ICT-related business functions, the associated information assets, and all potential sources of risk. Additionally, conducting regular ICT risk assessments, at minimum on an annual basis, plays a pivotal role.

The pursuit of digital operational resilience necessitates a **proactive testing regimen**. Regular assessments are crucial to identifying vulnerabilities, such as single points of failure and anomalous activities, thereby fortifying an organization's readiness to respond to disruptions and swiftly recover from incidents. This involves the establishment and consistent validation of dedicated ICT business continuity plans and ICT disaster recovery plans. Moreover, these plans should be subject to periodic testing and refinement to ensure their reliability. The regulation also advocates for robust third-party risk management concerning ICT. It proposes strengthening the existing outsourcing regulations that govern indirect oversight of third-party providers and encourages direct oversight of their activities when engaged by financial firms. The exchange of threat intelligence within the financial sector is promoted as an additional measure to enhance overall security.

Furthermore, an emphasis is placed on **fostering a culture of information and intelligence sharing**. This involves analyzing the root causes of incidents and assessing the effectiveness of protective and detection measures in place. To ensure responsible practices, communication plans are recommended for disclosing ICT-related incidents or significant vulnerabilities to clients, counterparts, and the general public. Notably, the inclusion of CSPs and considerations of portability are integral components of these initiatives, reflecting a holistic approach to digital operational resilience.

At its core, 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.

DORA's Impact on the Financial Services Industry

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: Work with CSPs. 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: Move workloads or data back to in-house data centers. Depending on the service, it is easier to move the application in-house than to make all the coding changes to move it to a different CSP. So, 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 (i.e., customer impact, which is what a regulator will care about) may be in-house.

DORA Challenges for Firms Heavily Relying on Non-EU CSPs

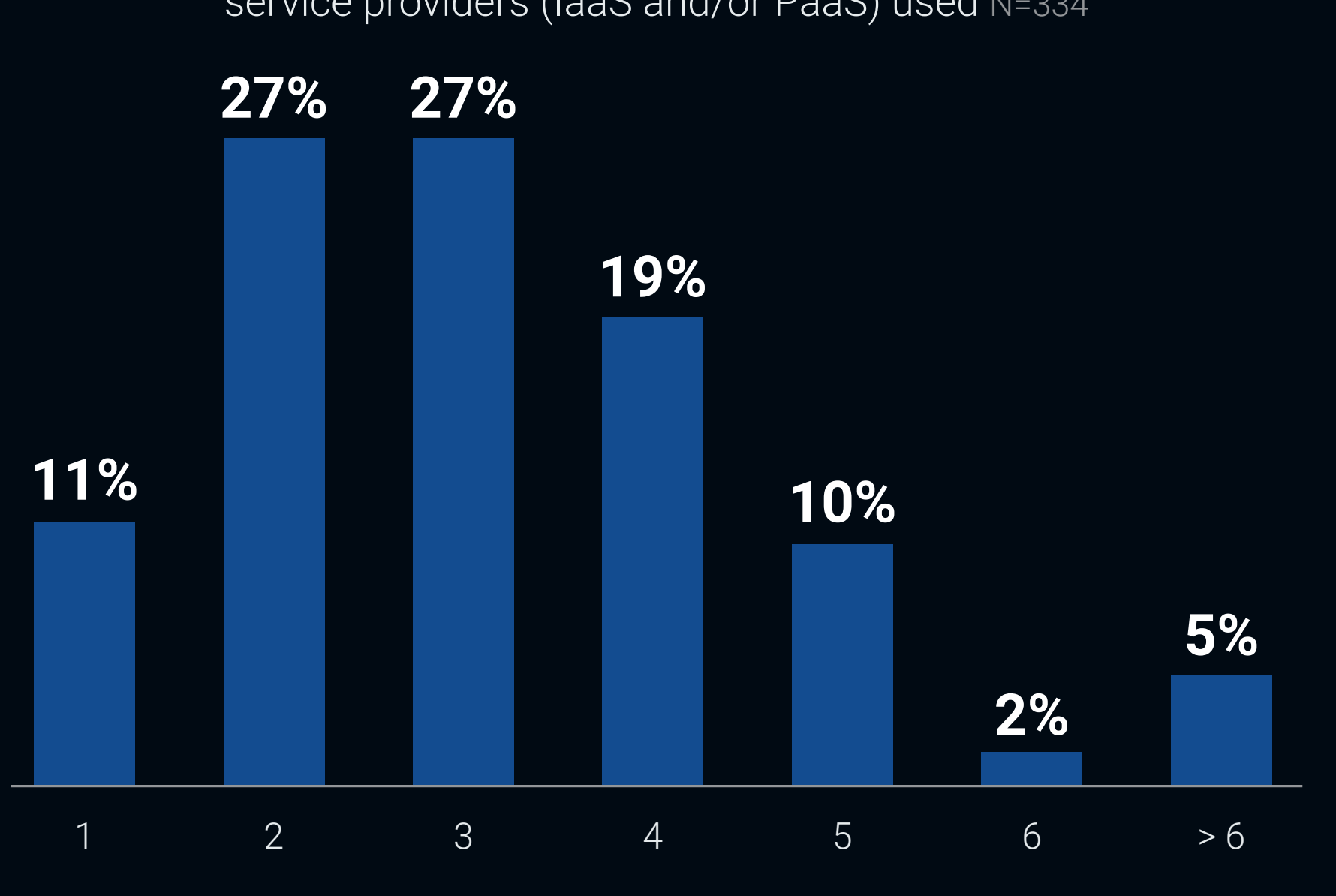
DORA underscores the necessity for organizations to reassess their strategies and explore avenues to alleviate the risks tied to third-party outsourcing. A potential approach for risk mitigation involves embracing an infrastructure conducive to a hybrid cloud strategy, incorporating portability as a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

90%

of organizations are already using multiple cloud service providers as part of their estate.

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.

Approximate number of unique public cloud infrastructure service providers (IaaS and/or PaaS) used N=334



How to Create a Cloud Strategy for Compliance

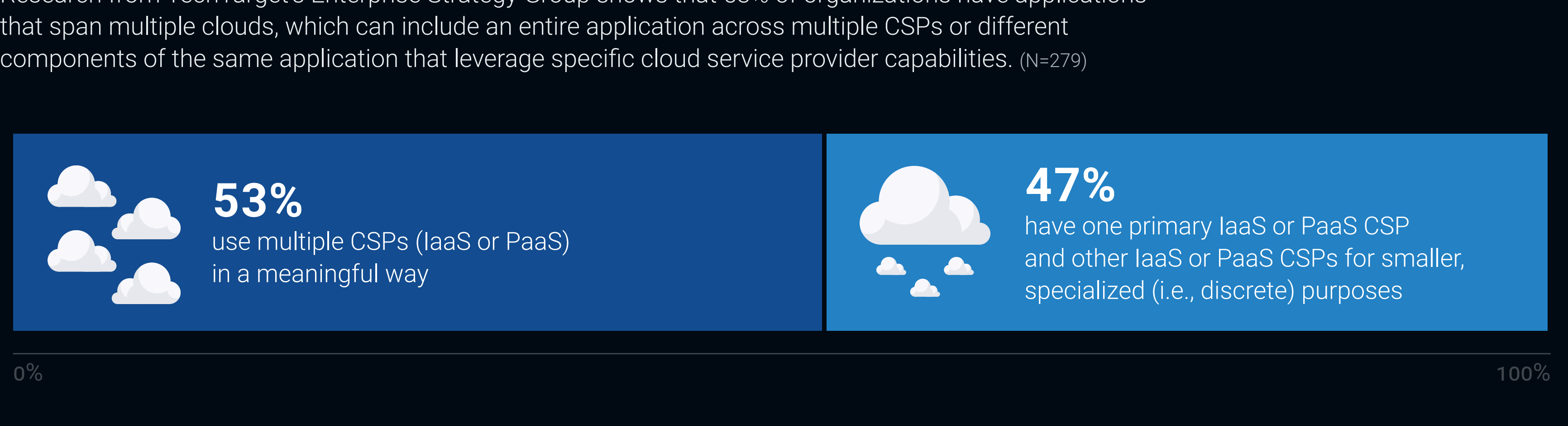
Incorporate a "cloud layer" into DORA stipulations, operating atop the chosen CSP or collaborating with a CSP that already employs such technology. This step aims to enhance provider independence, data security, and the ability to revert, typically encompassing foundational cloud services like security, 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 that demand tailored data compliance measures due to the nature of stored and utilized data—especially sensitive proprietary data—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.

Efficiency lies in foresight; this is where the value of OpenShift becomes evident. 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.

Research Shows Most Applications Span Multiple Clouds

Research from TechTarget's Enterprise Strategy Group shows that 53% of organizations have applications that span multiple clouds, which can include an entire application across multiple CSPs or different components of the same application that leverage specific cloud service provider capabilities. (N=279)



53% use multiple CSPs (IaaS or PaaS) in a meaningful way

47% have one primary IaaS or PaaS CSP and other IaaS or PaaS CSPs for smaller, specialized (i.e., discrete) purposes

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. Organizations should follow a best practice methodology such as the following:

DAY 1
Assess and plan the application-building journey.

DAY 2
Set up the necessary people, processes, and technology.

DAY 3
Deliver and operate first-mover applications.

DAY 4
Build capability and scale containerization across the organization.

Conclusion

As organizations adhere to DORA regulations, they need to be thoughtful about the steps for their cloud strategy. The strategy has to be an intentional—not accidental—adoption of a multi-cloud environment. 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 will 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.

Red Hat | Capgemini

LEARN MORE

Source: Enterprise Strategy Group Complete Survey Results, *Distributed Cloud Series: Application Infrastructure Modernization Trends*, March 2022.

Source: Enterprise Strategy Group Complete Survey Results, *Distributed Cloud Series: The State of Infrastructure Modernization Across the Distributed Cloud*, August 2023.

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.

Source: Enterprise Strategy Group Research Report, *Application Infrastructure Modernization Trends Across Distributed Cloud Environments*, March 2022.

Source: Enterprise Strategy Group Complete Survey Results, *Distributed Cloud Series: Application Infrastructure Modernization Trends*, March 2022.