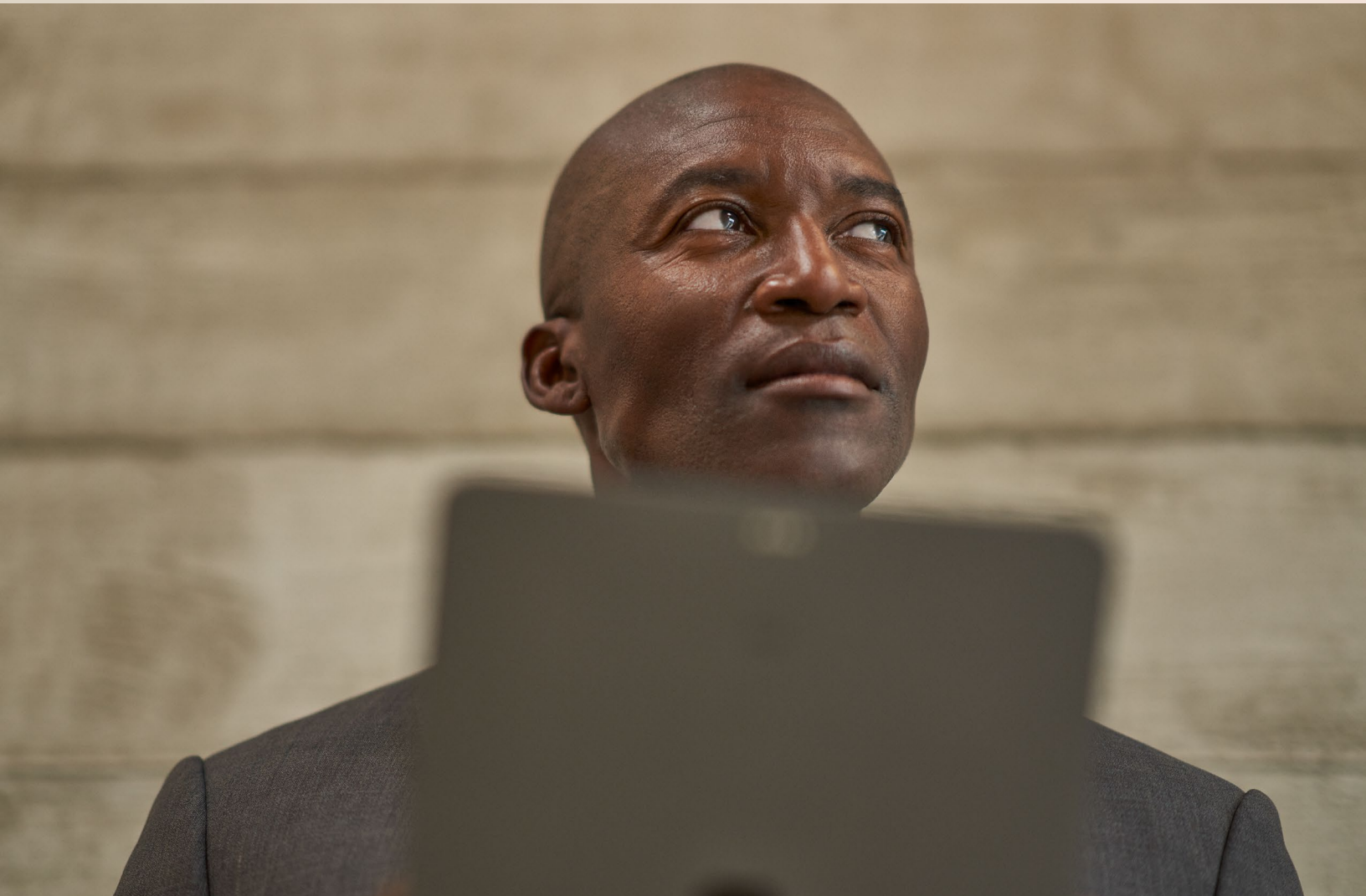
Microsoft

Operational resilience in action

Navigating DORA compliance with Microsoft



Operational resilience in action

Navigating DORA compliance with Microsoft

The Digital Operational Resilience Act (DORA) is here, having taken effect on January 17, 2025.[1] Is your financial services institution (FSI) ready?

Chances are that the answer is "no". Only about one-third of FSIs have done the work necessary to align with the new regulation.[2] As it turns out, DORA is very demanding, and with good reason. Strong operational resilience and the ability to recover quickly from any disruption or cyberattack is more critical than ever as banks, insurers, and other financial organizations modernize their infrastructure.

A European Union regulation, DORA applies to European FSIs—including banks, insurance companies, crypto-asset firms, and financial market infrastructures. It also applies to all doing business in the EU or with EU customers, and to critical third-party providers. It sets out stringent requirements for cybersecurity, operational resilience, and ICT (information and communication technology) risk management.

Although the regulation was announced back on January 16, 2023,[3] most FSIs aren't yet DORA-ready. Often, it's because of these challenges:

Legacy ICT infrastructure

Outdated systems prevail in the FS sector. Retrofitting or replacing them with the tools and technologies needed to meet DORA's mandates can be costly and difficult.

Third-party risks

FSIs often lack tools and processes to assess and monitor their supply chain risks.

Lack of compliance focus

DORA imposes greater expectations on managing ICT risk, and therefore using the right cloud technologies can help financial entities manage risk consistent with regulatory expectations.

High implementation costs

FSI entities—especially the smaller ones—are struggling to afford the technology, skilled personnel, and process upgrades that DORA requires.

Fragmented ICT and security

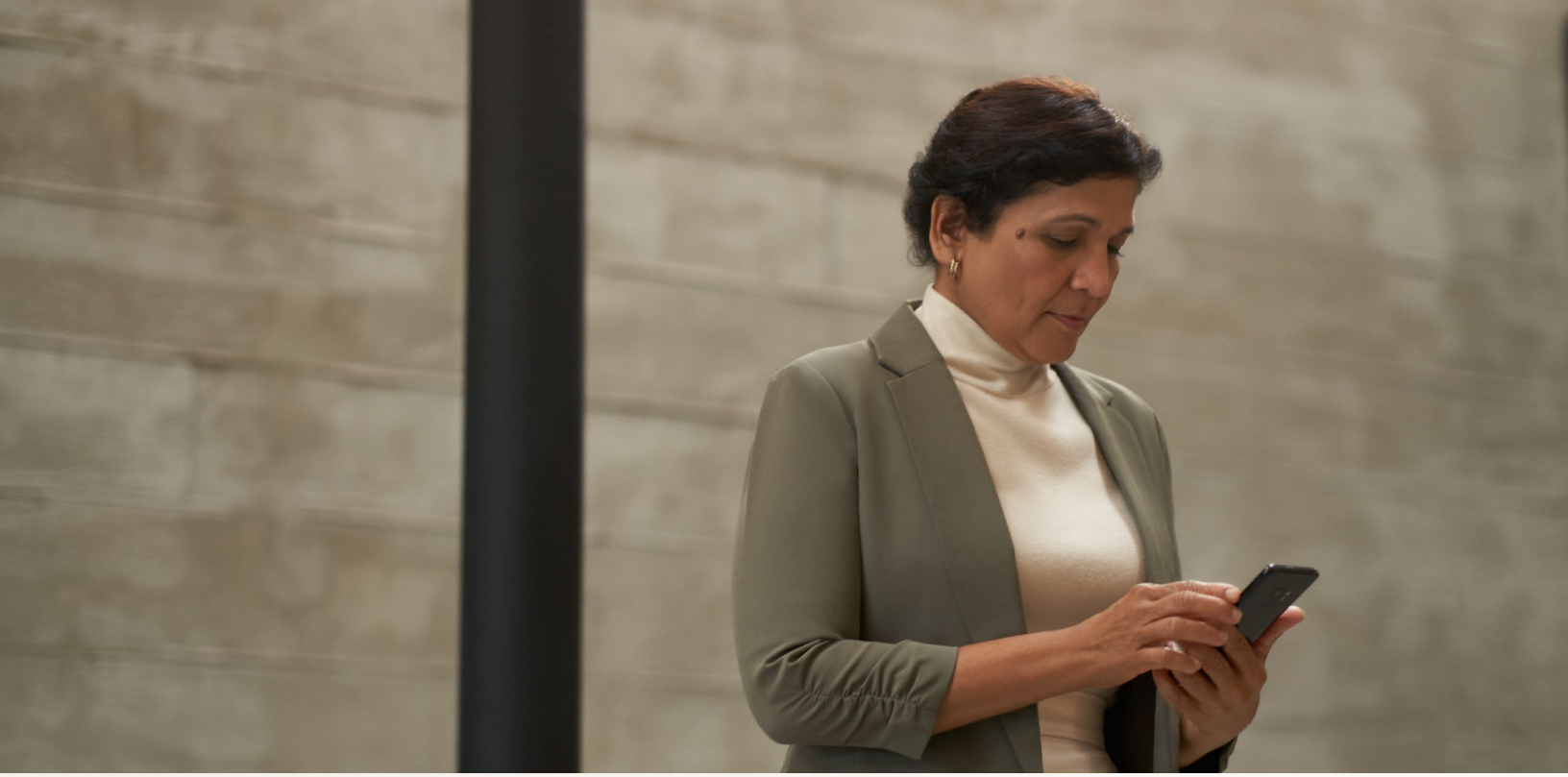
FSIs tend to provide their products and services as well as conduct internal operations using multiple platforms, leading to fragmented visibility and security protocols among departments and regions.

Formidable though these challenges might seem, they're far from insurmountable. Your FSI, whether a bank, insurance company, crypto-asset firm, or financial market infrastructure, can satisfy DORA's demands. Read on to learn how to build operational resilience in six steps.

When you've completed them all, your FSI will be able to operate with confidence that security is strong and that, should an attack occur, you can bounce back gracefully with minimal to no interruptions on your systems or services.

[1]Microsoft, What is DORA?, 2024.
[2]McKinsey & Company, Europe's new resilience regime: The race to get ready for DORA, 2024.
[3]EIOPA, Digital Operational Resilience Act (DORA), 2025.

Table of contents



Build operational resilience in six steps

The main imperative of DORA is that your FSI must build strong operational resilience and minimize concentration risk. Doing so is critical as cyber threats keep changing and digital dependencies become ever-more complex.

Concentration risk is defined as the potential for operational failure caused by heavy reliance on one or a small group of third-party service providers. When one vendor or supplier or an interrelated group provides a critical service or product, the risk goes up.

Operational resilience refers to the ability to recover from a cyberattack, outage, or other disruption with minimal to no downtime or interruption in services.

To strengthen operational resilience and reduce concentration risks, your FSI must identify and monitor critical third-party relationships and strengthen your risk governance and management, business continuity, and exit strategies, among other things.

The good news is you can strengthen your FSI's operational resilience in six steps.

STEP 1

Update cloud risk governance

DORA requires FS organizations to strengthen governance and risk management strategies, including for ICT service providers such as cloud providers. You'll need to identify, assess, mitigate, and monitor risks associated with your use of cloud services, and evaluate how well your cloud risk management framework ensures the confidentiality, integrity, availability and authenticity of information processing. You should revise this framework as necessary to keep your cloud risks under the threshold you've set.

Some questions to consider while reevaluating the framework include:

- Which of your cloud services are business-critical?
- What are the current and potential threats to your services?
- What is your institution's risk tolerance for these services? Your overall risk appetite?

Establishing a comprehensive cloud risk management framework is just the start. DORA also requires these capabilities and programs:

Third-party risk management (TPRM) strategy

Having an up-to-date TPRM strategy can help improve accountability and compliance from your cloud service providers (CSPs). Your organization's contracts with CSPs must comply with DORA and other relevant regulations and establish service-level agreements regarding data security, uptime, and incident management.

Real-time monitoring and visibility

Cloud monitoring will help you address your risks and predict future vulnerabilities. You can accomplish this with automation, AI, and tools that provide real-time visibility into your cloud environments.

Incident reporting and response

Your institution must develop incident reporting protocols for cloud-related disruptions and assess your cloud service providers' (CSP) incident response plans to establish that they can handle breaches or outages.

Resilience testing

Critical systems must undergo regular penetration tests, and in some cases, threat-led penetration testing is required. You should also perform scenario-based resilience testing, including simulated cloud outages and cyberattacks.

Global cloud security policies

Having a unified cloud security policy will help your institution consistently comply with DORA and local regulatory requirements. Global policies set the stage for evaluating incident scope, containing cyberattacks, and restoring critical systems, which are all essential for resilience.

Automated compliance and reporting

You'll need an automated, streamlined compliance process for cloud environments that generates audit trails and evidence for regulatory reviews, including DORA's.

STEP 2

Mapping dependencies

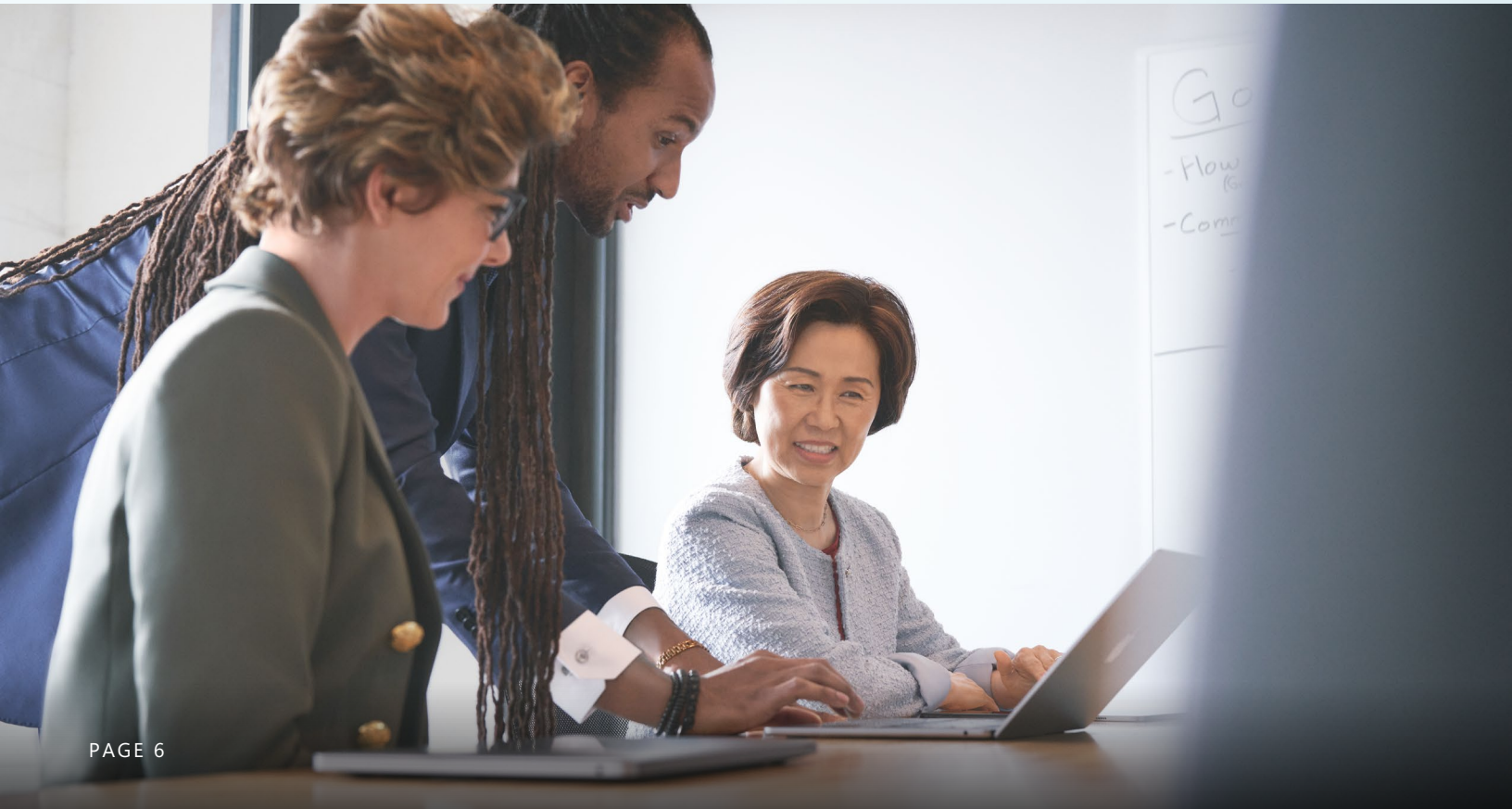
Mapping and understanding the dependencies among your business processes, ICT platforms, software, and third-party relationships is critical for operational resilience and DORA compliance. To gain a complete overview of your interdependencies, follow this guide:

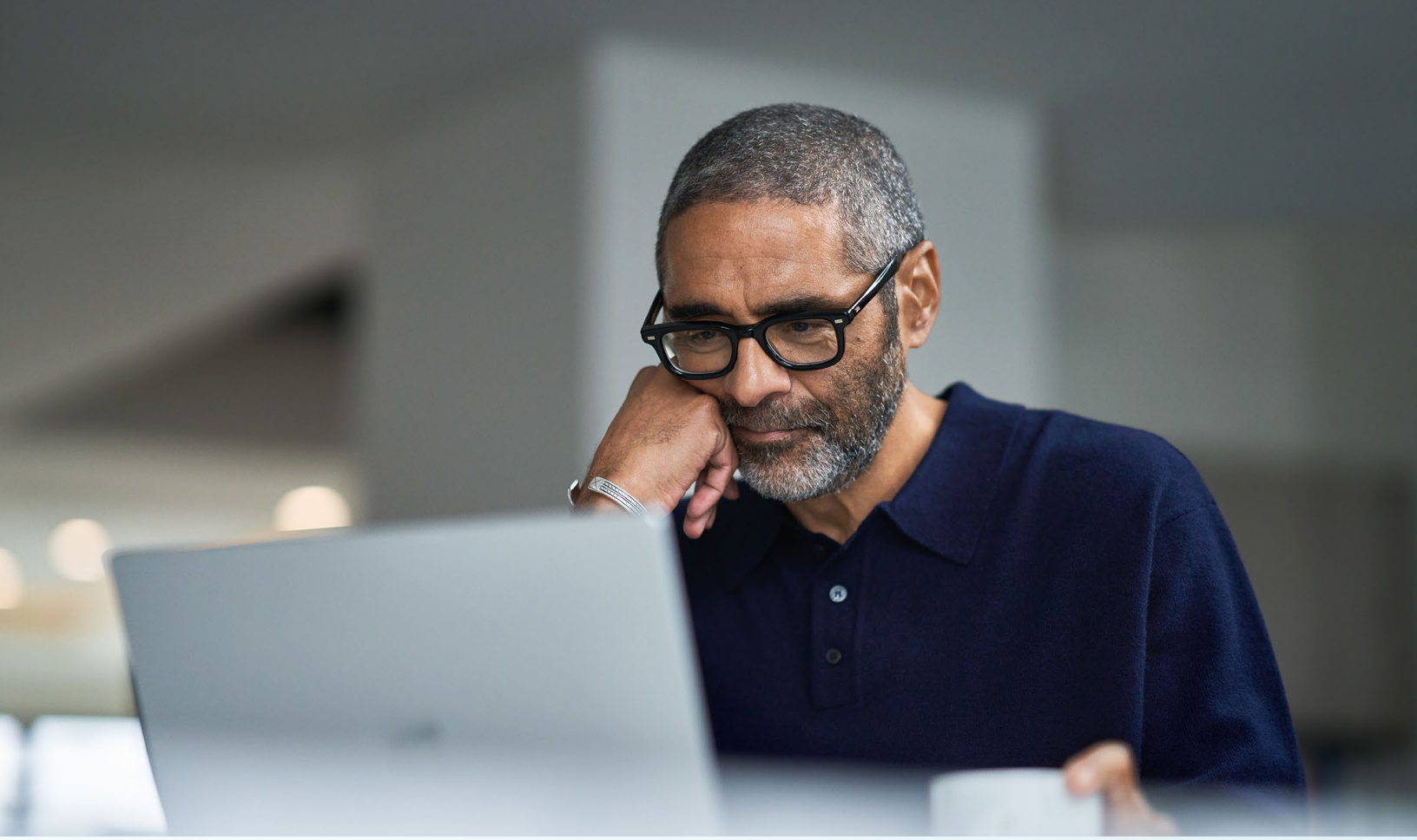
Dependency mapping exercise

You must identify and link the relationships between all your critical business processes, ICT platforms, software, and third-party relationships. IT asset management or configuration management database tools can be useful for scanning your infrastructure and identifying interconnected systems. Application performance monitoring tools help identify the real-time dependencies among your applications and platforms. You may also use a third-party risk management (TPRM) platform to gain insights into your vendor relationships and supply chain dependencies.

Understanding concentration risk

You must comprehend your ICT concentration risk if you are to manage it in line with DORA mandates. The amount of risk will depend on your organization's technological environment: whether it's using on-premises equipment or cloud infrastructure. Your cloud environments may comprise private, public, or a mix of cloud types from one CSP; a blend of on-premises and CSP use (hybrid); or two or more hosted by a variety of cloud providers (multi-sourcing).





Inventory and classify ICT services

Your entity must record all ICT assets, including hardware, software, cloud platforms, and network components, and classify them based on DORA's definition of critical or important functions. “Critical or important functions”, under DORA, are those that, if disrupted, would materially affect your FSI’s financial performance, services, activities, or regulatory compliance.

Conduct business impact analysis

You’ll next identify how critical each dependency is and its effects on the business. You must also identify every “single point of failure”—those parts of your system that would shut the entire system down in the event of a failure—plus all interdependencies among systems, software, and third-parties.

Risk assessment of dependencies

You must assess and understand the risks stemming from your ICT platforms, including downtime, cyberattacks, and data breaches. You must also identify and document outdated software libraries, as well as unsupported software versions and the risks they pose.

Integrate dependencies into enterprise risk management

Now, you must consider integrating your dependency maps into your enterprise risk management frameworks. Doing so will reveal insights into your risk profile, improve your risk management and response strategies, and—last, but not least—fulfill your DORA obligations.

Is your cloud environment increasing your risk?

Your ICT concentration risk is related to your cloud infrastructure. Each environment has its pros and cons. Let's take a look:

On-premises

Your organization has centralized its IT hardware, software, servers, storage, and networking equipment and manages it internally. Although no third-party is involved, concentration risk is higher due to:

Single point of failure

Critical systems' central location raises your vulnerability to natural disasters, power outages, and physical security breaches.

Bugs and vulnerabilities

On-premise software must maintain updates on security vulnerabilities and bugs, a process that depends on third-party vendor maintenance contracts creating similar third-party dependencies as with cloud but often harder to replace.

Limited scalability

Surges in demand may be difficult for your equipment to handle, hindering critical functions during peak periods.

Cloud infrastructure

Data storage, servers, databases, networking, applications, and tools reside in a remote location and are accessible via internet. One or more CSPs manage your cloud infrastructure; the amount and type of concentration risk depends largely on the model your institution uses. These include:

Public or private cloud

In a public cloud, a third-party provider serves as host to multiple customers. These environments are highly scalable, cost-effective, and accessible for any FSI. Private cloud means that hosting and services are exclusive to one user. Using a single CSP (whether public or private) brings a higher level of concentration risk, due to:

Single point of failure

Relying entirely on one CSP can offer greater simplicity and resiliency based on proper configuration and implementation. However, you're still vulnerable to disruptions stemming from outages and security breaches.

Limited control

CSPs usually offer standardized products.

Vendor lock-in

Exclusive use of a proprietary technology or service can make it more difficult to change providers. Assess interoperability of the services you use, termination rights to exit a service, and portability to another platform or on-premise.

Hybrid cloud

With this approach, you can use both on-premises data centers and cloud platforms to enjoy the benefits of each. Workloads are distributed across multiple platforms for optimal performance, cost efficiency, and compliance. Concentration risks include:

Single point of failure

Having many critical functions in a single location or cloud platform raises the risk of disruption caused by an on-premises or CSP outage.

Vendor lock-in

Dependence on a CSP or technology within the hybrid infrastructure poses supply chain risks and limits flexibility.

Inconsistent security policies

Managing security on multiple platforms can be challenging and may create security gaps.

Multicloud

In this model, you'd use services from two or more cloud providers, private or public, to benefit from the capabilities of each provider, optimize costs, and avoid relying on a single vendor. Through this model, concentration risk is lowered, but not eliminated, due to:

Vendor-specific dependencies

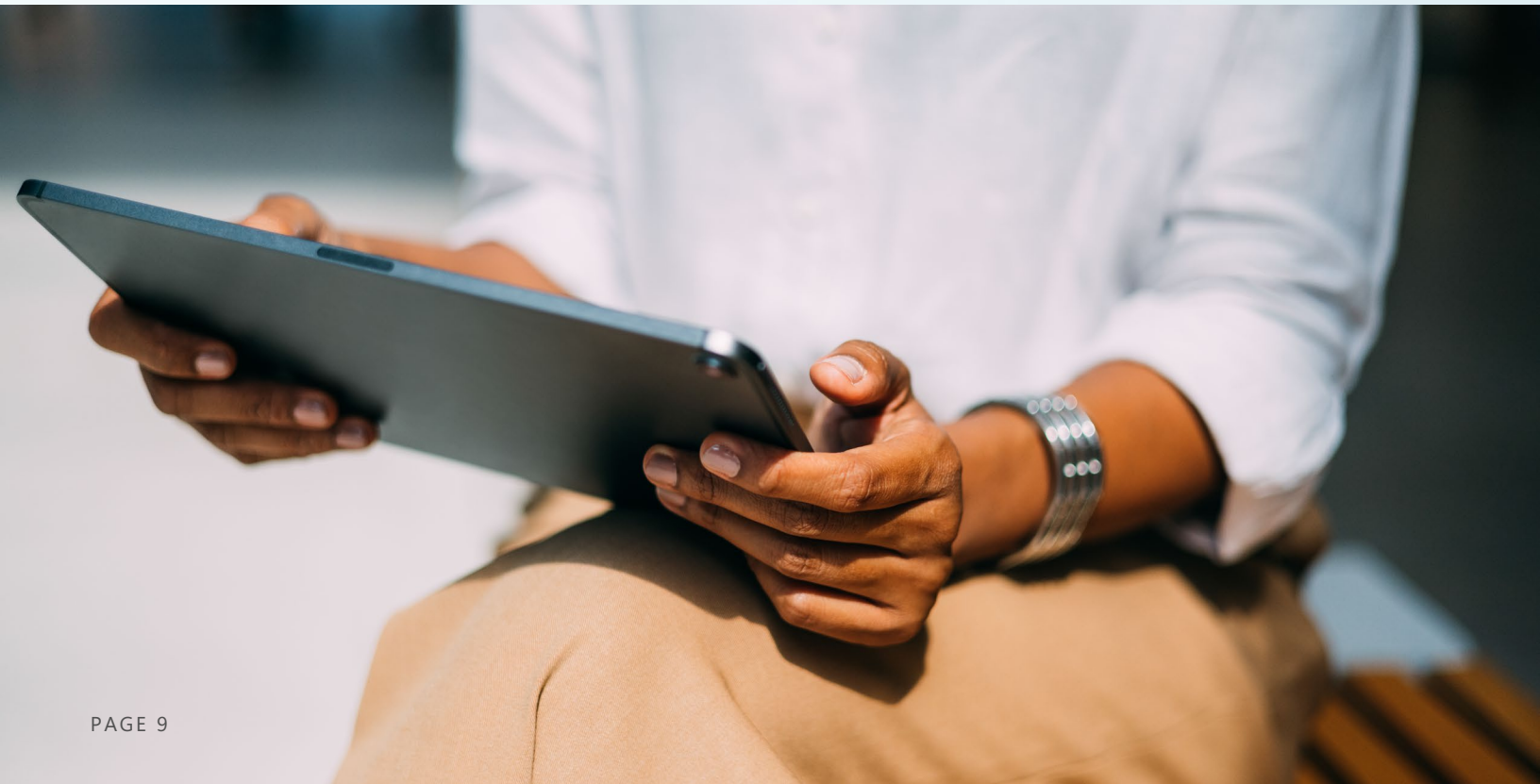
When your institution leans too heavily on one feature or cloud platform, it loses flexibility.

Inconsistent security

Each cloud platform has its own security measures, making it challenging for your security teams to maintain consistency.

Operational challenges

Managing multicloud environments increases complexity and does not necessarily increase resiliency.



STEP 3

Assess alternatives

Once you understand your organizational and system dependencies and their effects on your business, it's time to address the associated concentration risk.

Removing concentration risk altogether isn't usually possible. Your best strategy is to focus on finding alternatives and evaluating threat scenarios associated with your concentration risks.

To identify alternatives, ask these questions:

- What are the practical alternatives among on-premises, hybrid, multi-sourcing, and full cloud environments?
- What are the pros and cons of each alternative?
- How resilient are these alternatives?
- How do their risk profiles compare with one another?
- Which choice best fits our risk appetite and cloud strategy?
- In case of an exit: can and should the vendor exit completely?

When evaluating threats, you might weigh scenarios such as data center disasters, hardware failures, network outages, cyberattacks, faulty changes and upgrades, and human errors. Devise mitigation measures for each scenario, weighing costs, complexity, and resource availability. There is no one right answer or solution and design principals are flexible, and risk based. Devise measures which would enable the following:

Reduce the probability of the threat event

Craft risk management measures, including a Zero Trust security model, state-of-the-art infrastructure, periodic system updates, and the use of modular and open-source technologies.

Reduce concentration at lower levels

Design your services to operate in multiple availability zones, putting in place redundancies and recovery mechanisms such as backups and implementing geo-redundant designs.

Take action

- Learn about the responsibilities of FSIs under DORA with **DORA documentation**
- Access country-specific resources to understand how to meet requirements in the **Service Trust Portal**
- Get the framework to design and build well-architected cloud workloads with **Azure Well-Architected Framework**
- Accelerate security operations center response with **Microsoft Defender XDR**
- Unlock intelligence-driven incident response with **Microsoft Incident Response**

STEP 4

Design for resilience

Compliance with DORA will require changes to your ICT infrastructure. To reduce the risk of disruptions to your systems and operations while you make these changes, you'll need to design with security and reliance in mind. Here are the steps:

01

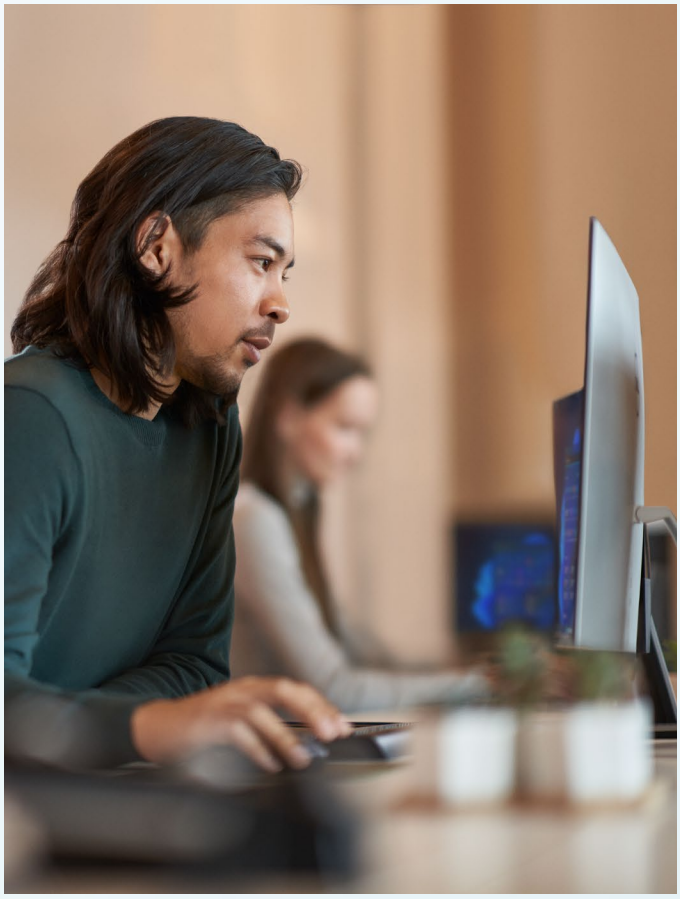
Build a resilient system architecture

To establish that your systems will perform without interruption, design them for redundancy and use data centers in a variety of locations so that no single point of failure can shut them down. Fault-tolerant designs will allow your systems to operate even if hardware or software doesn't.

02

Improve flexibility and scalability

To adapt to technological advancements without significant reworking, your ICT needs flexibility. To grow with your networks, it must also be scalable. Use modular components, microservices architectures, containerized workloads, and APIs to ensure portability and easy modifications.



03

Strengthen data protection and backup strategies

Plan for frequent backups of your critical systems and data. Encrypt data at rest and in transit, and store it in secure, geographically distributed locations. Create a comprehensive disaster recovery plan with recovery time and recovery point objectives so your organization can quickly respond to natural disasters, cyberattacks, and other unexpected events.

04

Build cloud-native solutions

Cloud-native solutions support greater efficiency, operational resilience, and innovation. Here are tips for design and implementation:

Choose the right cloud platform for your needs: Private cloud environments are best for industries with strict data compliance requirements. Factors to consider include security, scalability, integration capabilities, and compliance features.

Design cloud-native architecture: Use tools that help containerize newer and older applications and orchestrate scaling, load balancing, and deployment. For modularity and interoperability, develop applications and systems that communicate using APIs.

Modernize legacy applications: Redesigning your legacy systems into microservices or using a service-oriented architecture lets your services scale, deploy—and fail—independently, without affecting the rest of your system.

Use cloud-native technologies: Cloud monitoring tools can provide real-time visibility into your system's performance. Serverless platforms are ideal for designing flexible, cost-effective, and scalable applications.

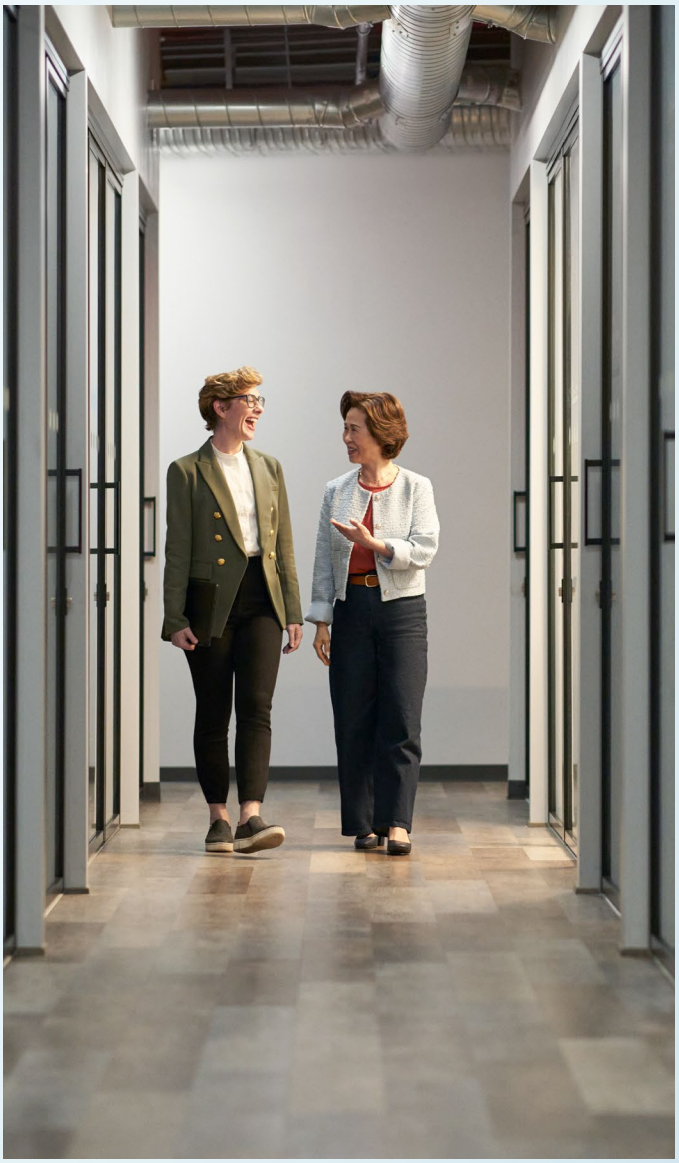
05

Improve identity and access management

An effective identity and access management (IAM) policy adds a layer of security for sensitive data, key for DORA compliance. A comprehensive IAM strategy will include:

Zero Trust architecture: Continuous verification on all systems and platforms will minimize the risk of unauthorized access.

Role-based access control: Grant least-privilege access according to job functions.



STEP 5

Test your business continuity plan

Having a business continuity plan (BCP) and testing it frequently is not only key for DORA compliance, but also essential for your FSI's operational resilience. When writing your BCP, be sure to plan for disruptions in third-party services such as from cloud services, payment processing, and IT infrastructure. Resilience means being able to weather these and other events without disastrous effects on your own services and operations.

Understanding shared responsibility in the cloud

Do you know who's responsible for the security of the cloud platforms your organization uses? The answer lies in the shared responsibility provision of your contract with your CSP.

In general, cloud providers mind the security of the equipment and grounds housing the servers and other equipment they own, while the users protect their data and applications in the cloud and any equipment on their premises.

Whatever the terms in your shared responsibility agreements, it's important to know and understand them. They should clearly define the following:

Security and compliance responsibilities

The underlying contract should clearly lay out obligations of the CSP and the financial institution from a security and compliance perspective, including: a clear and complete description of all functions and ICT services to be provided by the ICT third-party service provider, SLAs, commitments concerning protection of data, and termination rights and other obligations as required under DORA.

Data ownership and management

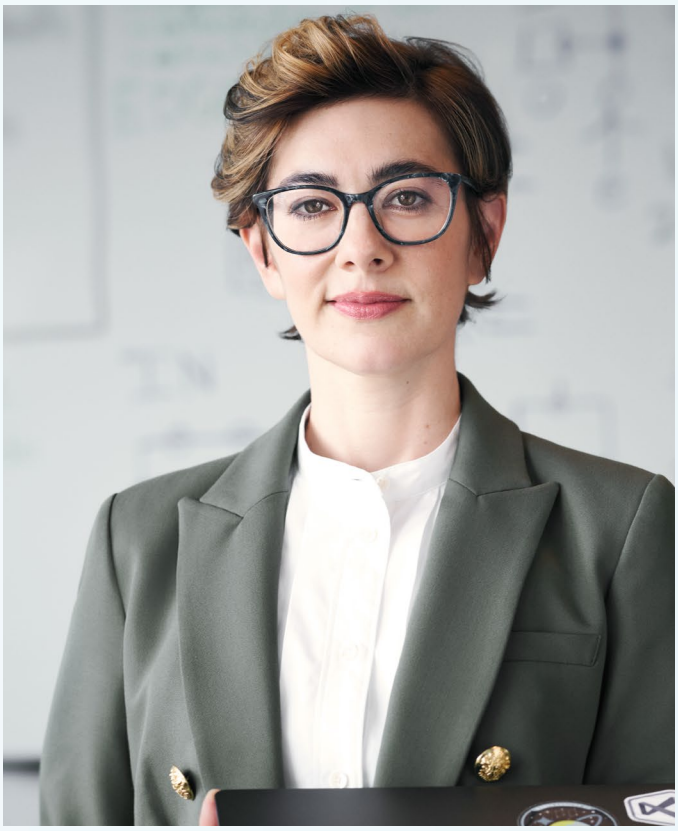
The FSI always owns the data. Your agreement should specify how the data will be stored, where it will be stored, how it will be processed and backed up, and should define protocols for deletion of customer data when the agreement comes to an end.

Service level agreements (SLAs)

The contract should specify both the SLA and the terms if the service provider does not achieve and maintain the service levels for each online service as described in the SLA, e.g., you may be eligible for a credit towards a portion of your monthly service fees.

Incident management and reporting

Clearly outline responsibilities for incident detection, notification, and escalation. It should also define how root cause analyses will be conducted and the collaboration process for resolution.



Disaster recovery and business continuity

DORA requires CSPs to act as trusted partners to FSIs in helping design detailed disaster recovery plans, outline data backup policies, conduct disaster recovery testing, and implement protocols to maintain services during outages and system disruptions.

Take action

- Learn how to develop a business continuity plan with **Microsoft Compliance**
- Accelerate your cloud adoption journey with proven guidance with **Microsoft Cloud Adoption Framework for Azure**
- Learn about Microsoft's contractual commitments under DORA in the **Microsoft Products and Services Data Protection Addendum (DPA)**
- Stay informed and act quickly on service issues with **Microsoft Azure Service Health**
- Gain insight into the overall health of your environment with **Microsoft 365 Health dashboard**

STEP 6

Prepare exit plans

DORA requires a comprehensive exit plan to address catastrophes such as bankruptcy or failure of an ICT third-party service provider. Complementary to your business continuity plan, your exit plan will help ensure a smooth transition when switching ICT service providers, where appropriate. Both your business continuity and exit planning commitments should be outlined in your agreement with your CSP. To design an exit plan for each contractual agreement with ICT providers, take these steps:

Map dependencies and critical functions

Having reached this stage, you will have already identified all dependencies and critical functions associated with the ICT provider, documented all the services, data, and infrastructure it provides, understood the relationship between their system and your internal systems, and classified priorities for each.

Define a step-by-step transition process

Define a notice period and transition plans for securely migrating all data to an alternative solution. Establish a service transfer process and, before making the transfer, test it to confirm that your operations won't be affected.

Define data retrieval and protection protocols

Your exit plan should always include contractual clauses establishing your FSI's data ownership. In addition to ensuring compliance during data migration, you should define protocols for deleting data from the outgoing provider's systems.

Testing exit plans

DORA requires FSIs to regularly test and maintain exit plans for all third-party providers. You'll need to test your exit plans annually and evaluate the performance of each element, including data migration, service continuity, and systems testing. Update your plans regularly to align with business needs.

Take action

- Help protect and secure multicloud and hybrid environments with **Microsoft Defender for Cloud**
- Get the most advanced set of governance capabilities of any cloud provider with **Microsoft Azure Governance**
- Reduce risk and complexity with unified data security, governance, and compliance solutions from **Microsoft Purview**
- Use intelligent insights and guidance to strengthen your organization's security posture with **Microsoft Secure Score**

How Microsoft helps customers

Microsoft is the leader in financial services compliance. For more than a decade, we have helped FSI customers meet their regulatory requirements.

As a critical third-party technology vendor, we understand DORA requirements and enable compliance with its applicable provisions. We'll support your FSI to help you do the same, aided by built-in ICT risk management capabilities that integrate with Microsoft cloud and enterprise solutions.

We'll help guide you swiftly and smoothly into DORA compliance in three areas:

Contracts

Microsoft works closely with our customers to ensure that contract terms align with the applicable DORA requirements. We have also added a DORA Addendum which covers the necessary contractual commitments.

ICT risks and internal governance

DORA requires your FSI to manage ICT third-party risk, set a policy on the use of ICT services supporting critical business functions, and maintain a register of information on all contractual arrangements with ICT third-party service providers. To ensure that you meet these requirements, Microsoft provides state-of-the-art ICT risk management capabilities with a variety of our products. You can find the key elements of our ICT risk management framework in the Microsoft Data Protection Addendum, Product and Service Terms, and Financial Services Amendment.

Incident management, classification, and reporting

Microsoft's tools for incident detection, investigation, reporting, and response plans help enable DORA compliance. Microsoft Azure Security Center, Microsoft 365 Health Dashboards, and Microsoft Defender are some of the tools which can help monitor your technology's status so you know whether it's working as it should and help you detect and respond to security incidents.

Microsoft

Ready to build strong operational resilience and achieve DORA compliance?

- Learn more about the Compliance Program for Microsoft Cloud
- Learn how to support your financial services organization
- Learn about hybrid and multicloud management solutions
- Contractual terms are available through your Microsoft contacts. Please reach out to them for further details.

Follow up with your account team to connect with a compliance expert.