Digital dependence of the financial sector

risks, resilience and European autonomy

DeNederlandscheBank
EUROSYSTEEM

AFM

Table of contents

Summary and key messages 3
Short term: preparing for disruptive scenarios 4
Longer term: strengthening strategic autonomy requires a European approach 4
Legislation and supervision 5

Introduction 6

1 The evolution of digital dependency risks 7
1.1 The financial sector runs on IT 7
1.2 Risks in digital dependency 9
1.3 Scenario analysis 12

2 Risk management at financial institutions and their IT suppliers 15
2.1 Awareness of dependency risks among financial institutions 15
2.2 Suppliers undertake initiatives to mitigate dependency risks 18

3 Supervision and policy 21
3.1 Current legal and regulatory frameworks 21
3.2 How to mitigate dependency risks 23

Summary and key messages

The financial sector is increasingly dependent on external IT service providers to support its core operations. Digital infrastructure now underpins almost all business processes, from customer engagement and risk management to compliance and transaction processing. Artificial intelligence (AI) is playing an ever more prominent role in these activities. A growing number of institutions are outsourcing parts – or even the entirety – of their IT functions to external providers, including cloud service providers, software vendors and AI model providers. This trend is driven by factors such as rising IT and cyber security complexity, rapid technological innovation and the pursuit of economies of scale. In particular, cloud services have expanded significantly in recent years, with an increasing share of institutions' technology stacks managed by third-party IT providers.

The growing digital dependence of the financial sector brings significant risks. Widespread reliance on the same providers and infrastructures has led to concentration and systemic risks. In recent years, a handful of global digital service providers – commonly referred to as hyperscalers – have come to dominate the market. Against the backdrop of heightened geopolitical tensions, there is a risk that state actors could exploit these digital dependencies for political leverage or weaponise them in trade disputes. Furthermore, complex chains of subcontractors and shared infrastructures mean that failures or cyber incidents at IT service providers can simultaneously impact multiple institutions. These opaque and interconnected supply chains create ecosystem risks that are difficult to manage. Vendor lock-in further complicates risk mitigation by making it costly to switch providers or diversify dependencies, thereby weakening institutions' bargaining power and increasing the likelihood of price escalation.

Financial institutions and IT vendors recognise these risks and are implementing measures to mitigate them. Institutions are developing exit strategies and continuity plans, and are mapping chain dependencies. Some institutions cite multi-vendor strategies, containerisation and the adoption of open standards as ways to enhance flexibility. However, these solutions remain costly and technically complex, making it challenging to avoid vendor lock-in. IT vendors, for their part, aim to ensure high levels of service continuity and reliability. Many are introducing sovereign cloud solutions, where data, services and management are governed by European laws and regulations. Yet, the effectiveness of these solutions in shielding against the influence of non-European actors remains uncertain. According to some institutions, technical measures such as in-house management of encryption keys can strengthen data security and continuity, but they do not fully protect against outages or data loss.

Short term: preparing for disruptive scenarios

In the short term, significant reliance on non-European IT service providers is a given. Institutions must take proactive measures to prepare for disruptive scenarios and minimise potential impacts. Sanctions or hybrid attacks could severely disrupt services.

- Collaborative efforts among institutions, IT vendors and authorities should focus on:
  - developing threat scenarios
  - sharing intelligence on concrete threats and attacks
  - conducting scenario-based chain testing, including real-life simulations.

  The AFM and DNB are willing to facilitate these collaborative efforts where needed.
- Institutions should be able to clearly articulate and justify how their decisions support data sovereignty and security, which may include leveraging non-European "sovereign cloud" solutions.
- By securing control over encryption keys wherever possible, institutions can prevent important and sensitive data from falling into third-party hands.
- Designing IT services with flexibility in mind could help reduce institutions' dependence. Recommended practices include containerising applications to enable vendor-independent deployment, adopting open standards and open-source solutions and engaging multiple vendors to reduce dependency risks.

Longer term: strengthening strategic autonomy requires a European approach

Over the longer term, it is important for Europe to reduce its dependence on non-European IT service providers and to work toward greater digital autonomy. Scenario analysis highlights the need for a stronger European technology sector – even under conditions of reduced geopolitical tension. Building a robust, innovative and autonomous European tech sector is advisable not only for resilience but also for safeguarding core European values such as privacy and inclusiveness.

Advancing digital autonomy extends beyond the remit of individual financial institutions and national financial supervisory authorities; it requires coordinated action at the European level.

- Addressing the structural drivers of digital dependency is essential. The Draghi report offers concrete recommendations to support this goal, that warrant follow-up.
- Reducing reliance on non-European IT service providers will require the development of fully fledged European alternatives. Financial institutions could consider adopting European solutions where they already exist. Pursuing these alternatives jointly can help overcome potential first-mover disadvantages and create the critical mass necessary to sustain viable European suppliers.
- In the field of (generative) AI, European applications are already available to financial institutions. Selecting these solutions can mitigate the risk of new vendor lock-ins.

- The AFM and DNB support the development of the European savings and investment union. For the evolution of the European IT sector, access to finance with a view to scaling up innovative companies is a key focus.

Legislation and supervision

Legislators and supervisory authorities have already introduced measures to address risks arising from digital dependencies.
The implementation of the Digital Operational Resilience Act (DORA) will strengthen control over risks to the continuity of service delivery related to digital dependencies, including the risk of cyber attacks on third parties and geopolitical threats. The DORA register of information enhances transparency around third-party dependencies, while its oversight framework subjects critical IT suppliers to a form of direct European supervision. Other – cross-sectoral – European regulations target major technology providers as well. These regulatory initiatives make an important contribution to managing third-party risks, although vulnerabilities persist.

The AFM and DNB:

- expect institutions to appropriately manage risks arising from third-party dependencies and will emphasise preparedness for disruptive scenarios in their supervision;
- consider it desirable for the relevant supervisory authorities – the AFM and DNB, as well as the Netherlands Authority for Consumers and Markets (ACM) and the Dutch Authority for Digital Infrastructure (RDI) – to intensify cooperation in supervising IT providers;
- will analyse the DORA register of information for the Dutch financial sector to identify concentrations in the use of IT services. Institutions are expected to use this register to properly identify their own concentration risks and dependencies;
- will examine the extent to which financial regulation (including DORA) and supervisory practice create barriers to selecting European IT providers or hinder innovation. Identified issues may prompt policy initiatives in the European context, engagement with legislators or adjustments to supervisory practice. This will allow institutions to consider the need for sovereignty against other characteristics when choosing their digital service provider;
- will ask European governments and supervisory authorities to evaluate whether DORA sufficiently enhances resilience to geopolitical risks and, if not, to consider issuing further guidance. In light of the geopolitical environment, they may in time consider the case for a cross-sectoral European cloud supervisor empowered to act decisively to mitigate digital-dependency risks – for example, by requiring adoption of truly sovereign cloud solutions;
- see opportunities to strengthen DORA as needed. Among other options, the third-party oversight framework could be made better enforceable, and more explicit requirements could be introduced for managing geopolitical risks, while maintaining sufficient scope for innovation.

Introduction

Technological innovation and digitalisation have fundamentally transformed the financial sector. Financial institutions are increasingly reliant on external technology providers, with banks, insurers and asset managers depending heavily on a small number of large – predominantly non-European – tech companies to support critical processes. Recent geopolitical developments and incidents have underscored the vulnerabilities inherent in this dependency. The sector now stands at a crossroads: while digitalisation is indispensable, it introduces new risks related to continuity, cyber security and even sovereignty.

The Dutch Authority for the Financial Markets (AFM) and De Nederlandsche Bank (DNB) view the reduction of the financial sector's reliance on non-European IT vendors as strategically critical. Dependence on one or a few providers creates systemic risk: a failure or incident at a major provider could disrupt large segments of the financial sector, threatening system stability and consumer interests. Identifying and managing these dependency risks is essential to maintaining a stable and resilient financial market. In the short term, opportunities to significantly reduce reliance on non-European IT suppliers are limited due to the absence of fully developed European alternatives. Institutions must therefore not hesitate in strengthening their digital resilience and mitigating dependency-related risks. Over the longer term, building a robust European technology sector will be key to reducing these dependencies, requiring timely and targeted action from both public and private stakeholders. This report sets out recommendations and follow-up actions by the AFM and DNB to support this objective.

This report is organised as follows. Chapter 1 outlines the current state of affairs, examining the extent to which the financial sector is intertwined with third-party information technology. It then analyses the key risks arising from these digital dependencies, identifying new vulnerabilities – from operational disruptions to strategic lock-in – and uses scenario analysis to illustrate how these risks could materialise in both the short and long term. In Chapter 2, the focus shifts to practice: based on interviews and analyses, insight is provided into how financial institutions and their IT suppliers deal with the identified dependency risks. Chapter 3 reviews the supervisory and policy framework. It summarises existing regulations and initiatives and sets out recommendations aimed at reducing dependencies and strengthening the digital autonomy of the financial sector.

1 The evolution of digital dependency risks

The financial sector is deeply reliant on information technology (IT) for its core processes, many of which are managed by external service providers. Digital infrastructure now underpins almost all business processes: from customer engagement and risk management to compliance and transaction processing. Increasingly, institutions are outsourcing parts or even the entirety of their IT functions to external suppliers. This trend is driven by factors such as rising IT and cyber security complexity, rapid technological innovation and the pursuit of economies of scale. This chapter examines how these dependencies have evolved (section 1.1), the risks that are emerging as a result (section 1.2), and, through scenario analysis, explores how these risks might materialise in the future (section 1.3).

1.1 The financial sector runs on IT

The digitisation of financial processes is driven both by the desire to execute processes more efficiently and with greater speed, and by external factors such as regulations and customer expectations. Digitalisation delivers significant benefits, including improved data quality, real-time insight into financial flows and automated reporting that supports informed decision-making. These technological advancements enable processes to become more scalable and flexible, which can improve international cooperation and enhance competitiveness. Customer interactions increasingly take place through apps, web portals and automated chat services such as chatbots and virtual assistants, while risk management and compliance functions are also heavily technology-driven. Rising expectations for speed, cost efficiency and service quality continue to accelerate the digital transformation. In response, regulators have imposed stricter requirements for transparency, accountability and risk management. However, greater reliance on IT introduces new vulnerabilities, such as cyber attacks and system failures, which demand robust security measures and effective incident response capabilities. This creates a reciprocal dynamic: IT is both a tool for meeting external requirements and a factor that influences the evolution of those requirements.

Increasingly, institutions are outsourcing parts or even the entirety of their IT functions to external IT suppliers. Institutions benefit from the expertise, innovation and economies of scale offered by specialised vendors, who can implement advanced applications more quickly and cost-effectively than in-house teams. Managing on-premises IT infrastructure entails risks and inefficiencies, such as ensuring physical security, backups and cyber resilience. By contrast, public cloud environments provide these safeguards through specialised providers, enhancing overall security and continuity. Outsourcing extends beyond supporting processes – it reaches the core of financial services. Institutions rely heavily on critical infrastructures such as public cloud platforms, secure data centres for data storage and hosting, networks for real-time transactions and advanced cyber defence systems. A 2022 survey by European financial sector supervisory authorities revealed that 9,000 of the 15,000 ICT service providers serving financial institutions were responsible for supporting critical or important functions.[1]

1 ESA 2023 22 - ESAs report on the landscape of ICT TPP's

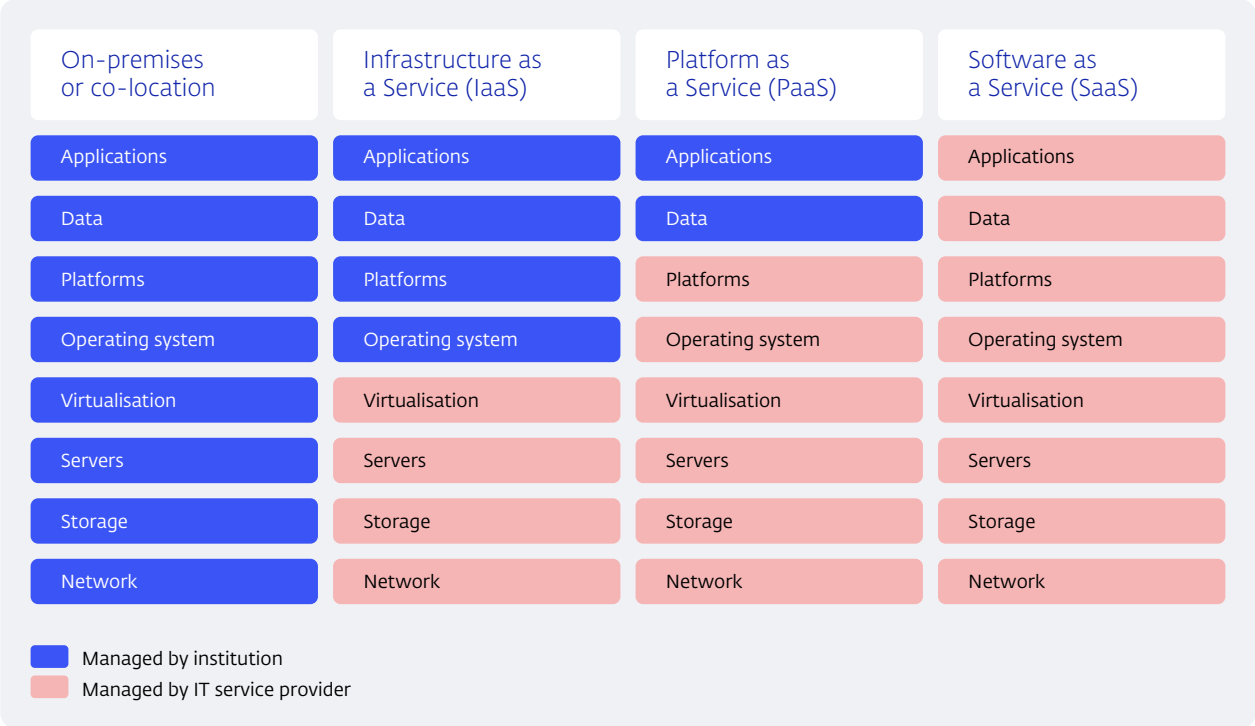
Artificial intelligence (AI) is playing an increasingly important role in financial institutions, enhancing efficiency, accuracy and customer focus. While traditional IT has primarily been used to automate processes and manage data, AI enables organisations to interpret and apply data in more sophisticated ways. This creates new opportunities to optimise operations, improve customer engagement and strengthen risk management. AI applications span a wide range of functions, including automated fraud detection, market and credit risk analysis, customer segmentation, transaction and incident monitoring and cyber resilience. Chatbots and virtual assistants deliver faster, more personalised customer interactions, while machine learning algorithms are able to identify patterns in vast volumes of financial data. Compliance processes also benefit from AI: anti-money laundering (AML) and Know Your Customer (KYC) requirements can be enforced more efficiently through intelligent data processing – provided that privacy safeguards are maintained and discrimination is avoided.

Cloud services have experienced rapid growth. The emergence of virtualisation technologies[2] have enabled a gradual shift from in-house data centres to cloud-based solutions. The promise of economies of scale, cost savings and accelerated innovation have made cloud adoption particularly attractive for less critical applications such as test environments and customer portals. Large US providers began offering standardised infrastructure services and quickly gained market dominance. This transition from internal IT environments to outsourced cloud solutions represents a significant development for the financial sector. While many institutions continue to operate on-premises data centres – sometimes in-house, but often through leased or shared facilities such as co-location – hybrid models that integrate external cloud environments are increasingly becoming the norm.

The transition from traditional on-premises IT infrastructures to cloud-based services reflects a structural change in how organisations manage and deploy technology. Within the cloud service delivery model, three primary forms are distinguished – Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS) – which represent an increasing degree of outsourcing and transfer of operational responsibility from the institution to the IT-service provider (see Figure 1). Institutions can select different levels within the technology stack for different processes, aligning the degree of outsourcing with risk and sensitivity. In some cases, financial institutions keep certain critical processes – such as core transaction processing or the management of sensitive customer data – in-house and isolated from the public internet. By contrast, less sensitive functions, such as email or HR systems, are often outsourced to cloud service providers. Other institutions pursue a full-cloud strategy, delivering most of their information services through cloud solutions. Many advanced capabilities are developed cloud-native, sometimes by the cloud provider but often by specialised vendors and are therefore available only as SaaS running on a public-cloud platform. In some cases, institutions can opt to run such capabilities on their own infrastructure or with an alternative cloud provider, but typically at higher cost or with reduced functionality.

2 Virtualisation technology enables a single physical computer to run multiple "virtual" machines, each functioning as an independent system. This approach maximises hardware utilisation.

Figure 1 Cloud-based service models



Alternatively, institutions can build their own services on a provider's platform (PaaS), or – where available – choose services that are not limited to a SaaS-only deployment model.

1.2 Risks in digital dependency

The growing reliance on external IT service providers and cloud environments within the financial sector results in concentration and systemic risks. Although many service providers operate in the market, the widespread use of the same infrastructures and vendors creates concentration risk. In recent years, a handful of digital cloud service providers – known as hyperscalers – have come to dominate the landscape, leveraging their scale, scope and broad range of services. Where institutions previously worked with multiple vendors, many now entrust their entire IT stack to a single

hyperscaler. This trend amplifies systemic risk, as the stability of the financial system increasingly depends on the resilience and availability of external IT suppliers. A failure or cyber incident at one provider can impact multiple institutions simultaneously. These dependencies extend beyond individual institutions and accumulate into system-level vulnerabilities, particularly through interconnected chains of service providers. Fallback and recovery mechanisms may prove inadequate if multiple parties share the same dependencies.

Similarly, the hardware underpinning IT systems is typically supplied by a limited group of non-European vendors. Servers, network components, security devices and storage systems often originate from a small number of global suppliers. Beyond these physical building blocks, many providers also deliver essential firmware and management software required for system functionality. Of particular concern is the emergence of specialised hardware for artificial intelligence. Dedicated chips are crucial for training and operating machine learning models, such as those used for real-time fraud detection or automated customer interaction. Production and innovation of such hardware are highly concentrated in specific regions, raising concerns about supply security, strategic dependency and technological sovereignty. Furthermore, reliance extends to the raw materials needed for manufacturing, creating additional layers of vulnerability.

Against the backdrop of heightened geopolitical tensions, there is a risk that state actors could exploit these digital dependencies for political leverage or weaponise them in trade disputes.[3] European financial institutions' heavy reliance on predominantly US-based IT vendors, including major cloud service providers, puts them in a position of vulnerability. One critical risk scenario assumes that non-EU IT service providers, under orders from state actors, could selectively cease, interrupt or downgrade services to their customers. This concern has prompted non-EU providers to develop sovereign cloud solutions tailored for the European market. While sovereign cloud services represent a viable mitigation measure, their development and implementation require substantial time and investment. Meanwhile, the threat and potential impact of these risks can materialise acutely in the short term. This dynamic creates a tension between the urgency of addressing these vulnerabilities and the slower pace at which structural solutions can be implemented.

The complexity of IT supply chains is growing, creating layered dependencies that are difficult to oversee. For example, a financial institution may purchase a technology platform from a fintech company, which itself operates on a different cloud platform and relies on application programming interfaces (APIs)[4] from additional third parties. Incidents affecting suppliers further along the chain can therefore have unexpectedly large consequences. Institutions depend on the speed and diligence of every link in the chain when responding to disruptions. This ecosystem risk is challenging to manage because visibility into underlying parties is often limited. While

3 See also: DNB, Resilience in turbulent times.

4 API: application programming interface – the technical connection between IT applications.

the financial institution remains ultimately responsible, it frequently lacks a clear view of the deeper layers and the critical role of certain providers. Even when institutions gain insight into their supply chain, they often have little leverage to influence the internal controls of these third parties.

Vendor lock-in poses a significant risk, as migrating or adopting multi-sourcing strategies becomes increasingly difficult the deeper an institution is embedded within a specific ecosystem. Applications and data are tailored to the technologies of a particular platform provider, meaning migration to another platform requires substantial investment and typically involves a costly, multi-year transition plan. Consequently, multi-sourcing – the parallel use of multiple suppliers – almost always proves too expensive and too complex in practice, making meaningful risk diversification challenging. A multi-vendor strategy, where critical processes are split between different providers, is used more frequently but only partially mitigates dependency risks. This imbalance shifts negotiating power toward suppliers, increasing the risk of price escalation and reducing institutions' leverage in contract negotiations.[5]

As digitalisation advances, cyber threats are becoming more frequent and sophisticated, with the potential for far greater impact than in the past. Whereas earlier attacks typically targeted individual institutions, an attack on an external supplier can now indirectly affect multiple institutions simultaneously. Financial institutions increasingly recognise that their cyber resilience is only as robust as the weakest link in their digital supply chain. The number of cyber attacks continues to rise, prompting authorities such as the AFM, DNB and the ECB to conduct voluntary TIBER (Threat Intelligence-Based Ethical Red Teaming) and ART (Advanced Red Teaming) tests. These exercises involve ethical hackers probing institutions and their suppliers for vulnerabilities. The introduction of the Digital Operational Resilience Act (DORA) has also mandated TLPT (Threat-Led Penetration Testing) for the largest and most critical financial entities. These tests increasingly include third-party (co-)testing.

Outsourcing data storage and processing to cloud service providers introduces challenges related to data protection, regulatory compliance and supervision. Financial institutions operate under strict privacy and security requirements, which is why the use of public cloud solutions can sometimes conflict with existing regulations. This creates legal risks, particularly when data becomes subject to non-European legislation. For example, the US CLOUD Act grants US authorities the right to request data from US technology firms, regardless of where that data is physically stored. This provision conflicts with European privacy standards under the General Data Protection Regulation (GDPR). Dependence on foreign infrastructure therefore represents a vulnerability – not only in terms of availability, but also in maintaining control over data access and determining which jurisdiction governs that data.

5 See also the ACM's market study on cloud services, which discusses in detail the (potential) flaws in the functioning of the cloud services market.

1.3 Scenario analysis

Even in the short term, the financial sector may encounter events where third-party dependencies create problems for institutions. Some adverse scenarios, while extreme, remain plausible. They are characterised by low probability but high impact and can materialise rapidly (see Figure 2). For example, it is conceivable that key IT suppliers serving financial institutions could be compelled by governments to discontinue services (Geopolitical Sanctions scenario). Similarly, these vendors may become targets of hybrid attacks, indirectly disrupting the financial sector (Hybrid Attack scenario). Such scenarios could trigger severe consequences both within and beyond the financial system. Although options for immediate action during such crises are limited, institutions can adopt mitigating measures in advance to strengthen preparedness. These include enhancing collaboration through information sharing, conducting joint exercises and jointly developing threat scenarios.

Figure 2 Rapidly materialising disruptive scenarios

Geopolitical sanctions

Key third party suppliers are forced to cease operations.
Impact: Massive disruption of financial services. Due to the lack of fallback options to EU-based data centres, it is not possible to sustainably support the core applications of financial institutions. For the majority of applications, there is no immediate alternative.

Potential short-term measures

Reversal: Begin migration to EU-sovereign cloud supporting a minimal viable organisation
Harmonise: Launch and engage in EU-wide IT standardisation and harmonisation platform
Formalise: Define intra-EU collaboration. Specify services delivered, identify responsible guarantors

Hybrid attack

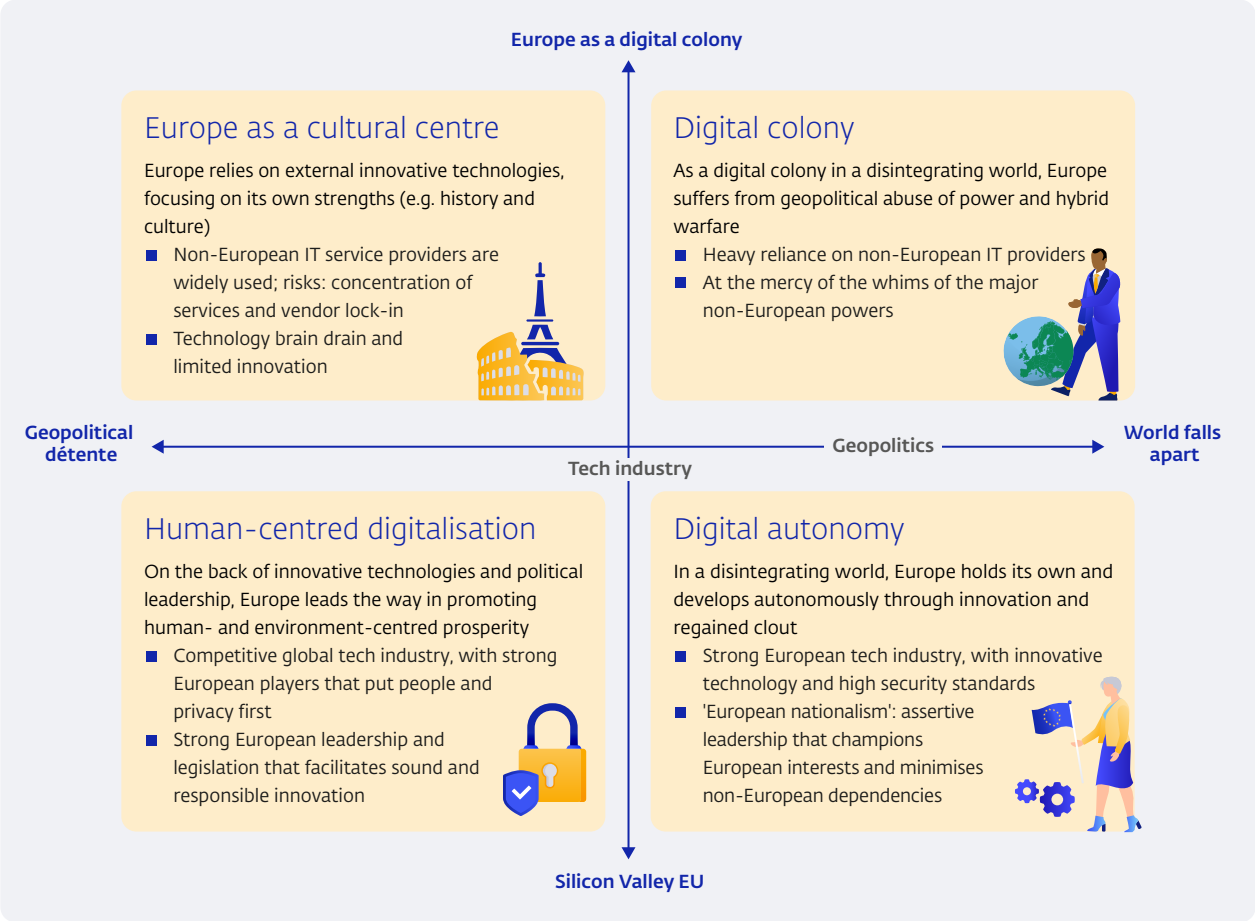
Intensive attack by state actor aimed at disruption. Cyber attacks and physical damage to critical infrastructure, for example attacks on utilities, leading to failure of critical technology suppliers.
Impact: Critical processes of financial institutions are disrupted.

Potential short-term measures

Collaboration: Share threat intelligence; conduct exercises jointly with providers (chain testing)
Scenario planning: Develop overarching threat scenarios with corresponding mitigation strategies
No-IT preparedness: Explore alternative data processing methods for IT-outage scenarios

Over the longer term, developments may lead to a range of possible scenarios. Geopolitical fragmentation could persist, with Europe's digital dependencies shaped by its ability to act. Conversely, a return to a less tense geopolitical environment cannot be ruled out. The IT services market may also evolve in different directions. Non-European players could maintain dominance, particularly in emerging technologies such as AI and, eventually, quantum computing. Alternatively, the European tech industry might strengthen – potentially accelerated by short-term disruptions – allowing European providers to emerge as major players over time. Figure 3 illustrates the potential long-term scenarios that could unfold.

Figure 3 Long-term dependency scenarios



The scenario analysis underscores the need for a stronger European technology sector. If geopolitical tensions escalate and Europe lacks a developed tech industry, it risks becoming a "digital colony," vulnerable to the influence of other global power blocs (Digital colony scenario). Conversely, by investing in its own robust tech sector, Europe can reduce digital dependencies and make the financial system less susceptible to disruptive events (Digital autonomy scenario). If geopolitical tensions ease but Europe's tech sector remains underdeveloped, dependencies on non-European providers will persist or even deepen, particularly in areas such as AI. Europe may focus on cultural leadership ('Europe as a cultural centre' scenario), leaving it exposed should geopolitical conditions deteriorate again. In a scenario where Europe succeeds in building a strong and innovative tech industry, this ecosystem can embed core European values such as privacy and inclusiveness ('Human-centric digitalisation' scenario). Financial institutions would then have viable European alternatives, reducing reliance on non-European providers. Achieving scenarios that enhance resilience and digital autonomy will require coordinated efforts from both public and private stakeholders. The next chapters address these actions in detail.

2 Risk management at financial institutions and their IT suppliers

Both financial institutions and their IT service providers recognise the risks associated with critical dependence on non-European technology companies. In the context of this report, we interviewed a range of financial institutions – including banks, insurers, payment service providers and asset managers – about how they manage technology-related dependency risks. We also spoke with various vendors, from global BigTech firms to specialised digital security providers. These suppliers have also recently made substantial investments in mitigating dependency risks, with particular emphasis on geopolitical vulnerabilities. This chapter provides a closer examination of the risk management strategies employed by financial institutions (section 2.1) and suppliers (section 2.2).

2.1 Awareness of dependency risks among financial institutions

Financial institutions state, as a starting point, that on the concentration of services among non-European hyperscalers is, to a degree, unavoidable. This is largely due to the current lack of European alternatives that match the quality offered by global providers. Although European cloud service providers do exist, they typically offer only basic services and fall short in advanced capabilities and scalability. In contrast, hyperscalers deliver global coverage, instant scalability, a high degree of redundancy[6], high security standards and access to sophisticated database technologies and analytical tools. Their platforms also host a wide range of innovative services from third-party providers. Europe's limited competitiveness in this domain is attributed to factors such as a weak innovation and investment climate, market fragmentation and regulatory barriers.[7]

While financial institutions deliberately choose US-based hyperscalers for the strategic advantages they offer, they are increasingly aware of the new vulnerabilities that accompany such dependencies. Directors and IT risk managers acknowledge a clear trade-off: modern cloud and software services deliver scalability, innovation and operational flexibility, but also shift IT support for critical processes outside the institution's direct control. Moreover, control over IT infrastructure is progressively migrating to external providers. Several major vendors are expanding their offerings "higher up the technology stack" – moving beyond basic infrastructure to deliver platform and software services. This deeper integration allows them to embed themselves further into the operational core of financial institutions.

Financial institutions are aware that this heightens their operational dependency. As a result, they carefully evaluate each outsourcing decision. While purchasing additional services from cloud providers may offer functional advantages and enhanced security, it also deepens vendor lock-in. To mitigate this risk, institutions are adopting open standards and containerisation technologies to improve workload portability and facilitate the migration of applications when necessary. Containerisation refers to the practice of packaging software applications into isolated, portable virtual containers, enabling them to run independently of the underlying IT infrastructure. Some institutions note that for latency-sensitive

6 Redundancy is defined as the deployment of additional capacity to ensure service availability and continuity in the event of outages.

7 For further context, see the Draghi report on EU competitiveness.

transactions – such as trading data, where rapid response times are critical – cloud solutions are often bypassed in favour of proprietary on-premise systems.

At present, financial institutions report limited operational dependence on generative AI technologies, but that can quickly change. These tools are primarily used to enhance employee productivity and streamline internal workflows. Institutions indicate that discontinuation of such tools would result in only a slight loss of efficiency, but would not disrupt core operations. However, the strategic importance of generative AI is expected to grow rapidly, potentially making it as indispensable as other foundational technologies. To avoid excessive reliance on non-European providers, institutions are actively exploring European alternatives – though the current market remains relatively underdeveloped. Continued growth and innovation in this sector will be essential.[8]

Where possible, financial institutions opt for multiple IT suppliers. However, the higher up the technology stack, the more difficult it becomes to diversify. Using two suppliers for hardware procurement is relatively straightforward and commonly practised. In contrast, cloud services often involve a single primary provider. Some institutions have adopted a dual-vendor cloud strategy, enabling rapid workload transfer between providers and significantly reducing dependency. Others have chosen not to pursue or have discontinued such strategies. While a multi-cloud approach can theoretically offer resilience, they find its practical implementation challenging, citing complexity and cost as key barriers. Larger institutions may engage multiple cloud providers, but typically for distinct application domains. This limits workload portability but helps distribute dependencies and strengthens negotiating positions. Smaller institutions often rely on a single primary cloud provider, supplemented by a limited fallback option – such as a private cloud or data centre. Redundancy is most commonly achieved within a single provider's infrastructure, for example by distributing IT systems across multiple data centre regions operated by the same cloud vendor.

For many financial institutions, shifting (or in some cases reverting) to in-house data centres or co-location ("on-premises") is not considered a realistic strategy. The complexity and cost of securing such environments against modern cyber threats are substantial, and many organisations no longer have the necessary expertise to do so effectively. Moreover, operating an in-house data centre does not eliminate external dependencies; institutions remain reliant on hardware suppliers, undersea cables and other critical infrastructure. Given these constraints, institutions are not attempting to eliminate dependencies altogether, but are focusing on actively managing risks within external partnerships. At present, this approach is viewed as more feasible.

Financial institutions apply intensive risk management practices to address technology dependency, with scenario analysis also playing a role. Technology dependency risks are a key part of the risk management strategy of financial institutions. These risks are embedded in periodic risk assessments and reflected in strategic IT planning. Institutions explore scenarios – such as prolonged outages or service discontinuation by

8 There are notable developments in this field. See, for example, ASML, Mistral AI enter strategic partnership, Nebul at the NVIDIA GTC 2025, and the European Commission's policy initiative AI Continent - new cloud and AI development act.

key providers – to prepare appropriate mitigation measures. Where possible, institutions are also open to sharing scenarios and insights from these exercises. While implementing mitigation measures can be challenging, the process of thinking through disruptive scenarios helps institutions clarify their remaining options and response strategies.

In line with the requirements of DORA, financial institutions are mapping the subcontractors and supply chain partners engaged by their primary IT service providers (see also Chapter 3). These insights enable larger institutions to incorporate specific provisions in contracts with major IT suppliers, including clauses promoting supply chain diversity and stipulations granting audit rights, which allow institutions to assess how providers safeguard their own continuity and security.

Financial institutions maintain exit and business continuity plans to address potential disruptions involving critical third-party providers. These plans outline procedures for transitioning workloads to alternative environments within defined timeframes, should one key technology supplier fail. The feasibility of such plans varies by domain. A loss of a major cloud provider would pose significant challenges, whereas switching from more specialised services may be quicker – assuming viable alternatives are available. In crisis situations, institutions could possibly accelerate transitions beyond what formal plans prescribe, temporarily bypassing standard procedures and governance to restore operations swiftly. To ensure effectiveness, institutions regularly test these plans and revise them based on the outcomes.

A scenario in which multiple major IT service providers simultaneously become unavailable to Europe – such as through geopolitical conflict – falls largely outside the scope of existing contingency plans. While the likelihood of such an event is low, its potential impact would be extremely severe. The economic interest of supplying technology services to Europe is considerable, which acts as a deterrent against using these services as geopolitical leverage. However, this risk cannot be entirely ruled out. Financial institutions also consider more realistic scenarios, such as the exclusion of a single company or individual from service provision due to sanctions, similar to the case of the Amsterdam Trade Bank bankruptcy.[9] Institutions aim to respond proportionally to such risks ; they weigh up the pros and cons and choose not to miss out on all the benefits.

In their risk assessments, financial institutions also qualify the broader implications of service disruptions. A failure involving a major hyperscaler would likely have a system-wide impact, affecting not only the institution itself but also its customers and the wider financial sector. The distinction is critical: isolated failures may pose unique challenges to individual institutions, whereas widespread outages affect many organisations simultaneously, meaning no single party is unduly burdened but amplifying societal and economic disruption. In such high-impact scenarios, a coordinated response is essential – one that involves financial institutions, IT service providers, government bodies and supervisory authorities.

9 DNB letter about ATB bankruptcy to the minister of Finance (in Dutch).

The sector therefore actively seeks cooperation and looks to the AFM and DNB for guidance in mitigating external IT risks and reducing dependencies over time. Almost all financial parties emphasise the importance of sharing knowledge and preparing jointly to manage dependency risks. They advocate the exchange of scenarios and best practices in the area of third-party risk, as everyone ultimately faces similar challenges and works with the same suppliers. A significant number of interviewees state that the AFM and DNB can play a facilitating role and help organise cooperation to address dependencies. Cloud services in particular are regarded as a "commodity" that can be effectively developed at a European scale. Achieving scale is seen as a greater challenge than securing investment capital. More can be accomplished collectively in this area. DNB and the AFM could support these efforts in a spirit of community building and coordinate joint supply chain tests, in which financial institutions and their key IT suppliers rehearse a scenario. There is a strong need for public-private partnerships.

At the same time, institutions want European rules and standards to remain pragmatic: their call is to focus on what is truly necessary. Some institutions point out that DORA creates incentives that may lead to increased concentration among service providers. They report having observed that smaller IT suppliers are withdrawing from the financial sector because they are either unwilling or unable to comply with all requirements following from DORA. This raises the risk of large, established IT vendors becoming even more dominant. Institutions also note that DORA encourages the use of fewer providers, meaning services are more often sourced from a single supplier rather than from multiple ones: "the fewer providers, the less paperwork." This does not promote diversity, and therefore undermines resilience. According to institutions, DORA and other legislation should be applied flexibly and proportionately, tailored to different types of institutions and focused on practical implementation. Unintended side effects should be minimised, for example by standardising requests for proposals. Clear definitions should also be used to avoid varying interpretations. The AFM and DNB agree with most of these points.

2.2 Suppliers undertake initiatives to mitigate dependency risks

Major technology providers recognise that the financial sector is highly dependent on them and are taking measures to enhance digital sovereignty. Some suppliers are experiencing pressure from their customers to take action. In particular, customers in the financial, defence and other sectors where availability and data security are critical are increasingly raising concerns about geopolitical risks. Prompted also by the entry into force of DORA, they demand contractual uptime guarantees, exit options and audit rights. Suppliers are responding to this and are actively seeking ways to strengthen customer confidence in data security.

Several cloud service providers offer financial institutions the option to procure services through separate legal entities based in Europe, commonly referred to as European sovereign cloud solutions. While the exact set-up varies by provider, these solutions generally involve operational and legal frameworks that fall under European jurisdiction and are designed to be as independent as possible from the non-European parent company. To comply with European laws and regulations on data, service provision and

management, providers may establish local subsidiaries, appoint European-based teams and implement governance measures that limit the influence of non-European legislation. In some cases, contracts explicitly prohibit key personnel from taking instructions from outside the EU. A critical requirement is that all data remains within EU borders and is managed exclusively by European teams. Sovereign cloud offerings can take various forms, including: running workloads locally at the financial institution with cloud infrastructure support, partnering with European firms to deliver cloud services, creating fully separate cloud regions within Europe and deploying isolated cloud environments that temporarily operate autonomously in local data centres, disconnected from the internet and vendor oversight. Although these solutions are primarily used in sectors such as defence, national security and government, interest from the financial sector is growing. However, these models often come with trade-offs in terms of resilience, functionality and cost.

These sovereign solutions are intended to provide assurance that non-European state actors and decision-makers cannot influence how services are operated. To achieve this, cloud providers implement legal, operational and organisational partitions designed to withstand external pressure – for example, in cases involving foreign data access requests or geopolitical incidents (often referred to as a "red-button scenario"). Cloud providers claim they will pursue legal avenues to reject such requests when they arise. However, it remains uncertain how effective these measures truly are in shielding services from the potential influence of non-European actors.

Cloud service providers are enhancing customer control over data by allowing institutions to manage their own encryption keys. These keys are used to encrypt the data entrusted to the providers. Instead of relying on the cloud provider, customers can choose to manage and securely store their keys in their own hardware security modules (HSMs). Alternatively, they may outsource HSM services to a specialised provider. By outsourcing customer-managed keys, the cloud provider does not have unauthorised access, and the associated data cannot be involuntarily transferred in unencrypted form to non-European actors. However, this approach places full responsibility on the institution to generate, secure and retain the keys – introducing significant complexity and risk. Moreover, this measure only protects data privacy, particularly in relation to legislation such as the CLOUD Act. It does not safeguard against other risks, such as service unavailability, data corruption or data loss.

Cloud service providers ensure high levels of service continuity so the highest level of reliability is achieved. Recognising the serious consequences of outages, major providers invest heavily in prevention and rapid recovery capabilities. Redundancy is a key focus: critical components – including undersea cables – are duplicated as a minimum and distributed across multiple geographic locations. Providers offer extensive fallback options, enabling systems and data to be quickly transferred to alternative data centres, either within the same region or across borders, in the event of a disruption. This infrastructure helps maintain service availability even during major incidents. For financial institutions, it is essential that these fallback procedures are regularly tested and supported by clear agreements on maximum recovery times and data integrity. Large cloud providers

typically offer a (much) higher level of built-in redundancy than individual institutions could achieve independently. As a result, they argue that the likelihood of a complete service failure is low, given the robustness of their infrastructure. In addition, they conduct continuity testing to ensure preparedness for emergencies.

Cloud service providers offer various options to support workload portability, including open standards, container technologies and multi-cloud architectures. Despite these tools, migrating critical IT workloads between providers remains complex and demands deep technical expertise, careful coordination and a strong focus on maintaining continuity. Adopting open standards, open-source software and interoperability can improve portability, but trade-offs remain. Conversely, the more extensively a financial institution uses a provider's full suite of PaaS and SaaS services – benefiting from rapid development, reduced administrative overhead and abstraction from infrastructure – the more constrained its ability to move workloads becomes. This calls for a careful balancing act, where institutions must avoid underestimating low-probability risks and long-term strategic considerations.

Measures taken by non-European suppliers help mitigate geopolitical risks related to availability and data security, but they cannot eliminate these risks entirely. Both financial institutions and non-European technology providers acknowledge that, despite their efforts, residual risks remain. Dependency persists: institutions continue to rely on external vendors to support critical IT processes, even with safeguards in place. Vendor initiatives primarily focus on enhancing customer sovereignty, but understandably place less emphasis on reducing vendor lock-in. To counterbalance this, financial institutions may choose to prioritise workload portability. However, actual fallback options in the event of prolonged outages remain limited – migrating to another platform or proprietary environment is often time-consuming and technically complex.

3 Supervision and policy

Legislators and supervisory authorities are placing increasing emphasis on enhancing digital resilience and autonomy within the financial sector. Geopolitical tensions have significantly increased the likelihood of disruptive scenarios, making preparedness a priority for both financial institutions and public authorities. In the longer term, reducing dependence on non-European IT service providers and strengthening digital autonomy is essential. This chapter begins with an overview of the current legal and regulatory frameworks relevant to digital autonomy (section 3.1), highlighting that these frameworks are not always sufficient to effectively manage dependency risks or support long-term autonomy. It then presents suggestions from the AFM and DNB (section 3.2) for follow-up actions aimed at improving resilience and at strengthening control over digital processes by reducing digital dependencies through a coordinated European approach.

3.1 Current legal and regulatory frameworks

In recent years, EU legislation aimed at managing IT and third-party risks has been strengthened. For the financial sector, the most notable development is the European DORA regulation, which entered into force in January 2025. DORA applies across the European financial sector and is designed to enhance the digital resilience of financial institutions. In the Netherlands, the AFM and DNB supervise compliance with DORA.

A core element of DORA is the management of risks associated with the use of IT services provided by third parties. The regulation emphasises that financial institutions remain fully responsible for the financial services they provide, regardless of external service providers involved. DORA sets specific requirements for third-party contracts, including provisions for exit strategies and continuity of IT services supporting critical financial operations. Institutions are also required to consider the impact of restrictive measures – such as embargoes or sanctions – in their risk analyses, as these may affect either the provider's ability to deliver services or the institution's ability to obtain them. Additionally, DORA includes regulations on the design of information security, applicable to both in-house systems and outsourced IT services. Periodic resilience testing, including ethical hacking exercises, is also a key component of the framework.

Under DORA, financial institutions must assess third-party dependencies beyond their own direct contractual relationships. They are required to maintain a register containing detailed information about the entire chain of IT service providers – known as the DORA Register of Information. Institutions are expected to use this register to properly identify their own concentration risks and dependencies. At the European level, the three financial supervisory authorities – EBA, EIOPA and ESMA – use these registers to determine which IT suppliers are most critical, based on factors such as systemic impact and the number of systemically important financial institutions they serve. In the Netherlands, the AFM and DNB will also begin analysing these registers to gain deeper insight into institutional dependencies and potential concentration risks as part of their supervision of the Dutch financial sector.

The most critical IT service providers at the European level will be brought under an oversight framework based on DORA. As a result, these IT providers will be subject to a form of direct European supervision starting in 2026. The oversight framework aims at evaluating how these providers manage IT risks which they may pose to financial institutions. When necessary, supervisory authorities – referred to as overseers –may conduct inspections and issue formal recommendations. In cases where a critical IT provider fails to comply, financial institutions may, in exceptional circumstances, be required to discontinue the use of specific services from the provider in question.

For financial institutions not covered by DORA, alternative regulatory frameworks are in place to mitigate risks associated with the use of IT services. A small subset of these institutions – which are not directly supervised by the AFM or DNB – fall under the oversight of DNB in its role as a central bank. This oversight is guided by international standards, notably the Principles for Financial Market Infrastructures (PFMI), and within the EU, the oversight framework for electronic payment instruments, schemes and arrangements (PISA), derived from these principles. As these standards are formulated at a relatively high level, institutions often align their implementation with the more detailed requirements set out in DORA. Additionally, for certain financial entities such as settlement agents and basic insurers, which also fall outside the scope of DORA, the Financial Supervision Act (*Wet op het financieel toezicht – Wft*) imposes obligations regarding the organisation of operational management, including outsourcing risks. These include demonstrable sound and ethical operational management, including clear segregation of duties and robust risk management practices.

Beyond financial sector-specific regulations, broader European legislation also addresses digital resilience and the role of major IT service providers. Since September 2025, the Data Act has been in effect, with oversight by the Authority for Consumers and Markets (ACM). One of its key objectives is to promote interoperability among cloud service providers, thereby lowering barriers to switching vendors and enabling a gradual transition of services to alternative providers. These provisions are designed to reduce the risk of vendor lock-in. In the area of information security, the Network and Information Security Directive 2 (NIS2) is now in force, regulated by the Dutch Authority for Digital Infrastructure (RDI). NIS2 aims to strengthen digital resilience across various sectors, including several types of financial institutions. For personal data protection, the General Data Protection Regulation (GDPR), overseen by the Dutch Data Protection Authority (AP), sets out rules for third-party data storage and processing, as well as strict conditions for transferring personal data outside the EU. The various supervisory authorities involved in these frameworks collaborate closely.

European and national legislation is further supported by guidance from financial regulators such as the EBA, EIOPA, ESMA and the ECB. These bodies provide additional guidelines, frameworks, toolkits, and Q&As to assist financial institutions in the responsible deployment of IT services, including cloud services. A notable example is the ECB Guide on Outsourcing Cloud Services. In addition, the Dutch professional association for IT auditors has introduced the International Digital Reporting Standards (IDRS), which aim to establish a consistent framework for organisations to report on their digital processes and IT risk management practices.

Although current regulations and additional guidance make an important contribution to managing third-party risks, vulnerabilities remain. The concentration of services among a limited number of IT providers and the persistent threat of vendor lock-in are not yet adequately addressed by existing regulations. This concern applies not only to reliance on predominantly non-European vendors but also to potential European alternatives. As financial institutions increasingly outsource critical business processes and data to external IT service providers, they relinquish a degree of direct control. This shift heightens exposure to disruptions stemming from geopolitical tensions, trade disputes or unexpected market developments – each with a direct impact on the reliability and security of their digital services. These risks are tangible and demand concrete, structural responses. It is therefore essential to accelerate investment in alternatives that enhance Europe's digital autonomy and resilience, while maintaining vigilance against new concentration and lock-in risks.

3.2 How to mitigate dependency risks

Mitigating the risks associated with disruptive scenarios and reducing dependency on third-party IT service providers requires a broad and coordinated set of actions. While some measures can be implemented in the short term, others require a longer timeframe and will yield results only over time. The urgency to act now is clear.

In the short term, significant reliance on non-European IT service providers is a given, which requires institutions to take proactive measures to prepare for disruptive scenarios and minimise potential impacts where possible. Compliance with DORA requirements is a key element in strengthening digital resilience. In addition, institutions should anticipate risks arising from geopolitical developments. One effective approach is to develop threat scenarios in collaboration with other institutions and relevant authorities. Where feasible, sharing information on concrete threats and attacks, both within the sector and with regulators, is strongly recommended. Based on extreme but plausible scenarios, institutions, IT vendors and public authorities can jointly conduct chain tests and real-life simulations. These exercises provide a valuable foundation for identifying and reinforcing mitigation strategies. Although such collaborative efforts are already underway, it is advisable to place greater emphasis on geopolitical risks and to involve IT service providers more actively. The AFM and DNB are willing to facilitate these collaborative efforts.

Additional measures can help mitigate the impact of adverse scenarios, even in the short term. Financial institutions could, where feasible, begin implementing a multi-vendor strategy. It is important that institutions have a clear understanding of which alternative suppliers are available to support critical services. Exploring the use of open standards and open-source solutions is also recommended, as these approaches reduce vendor dependency and enhance flexibility in deploying third-party IT services. Other technical measures such as containerisation enable workloads to be moved flexibly across platforms from different providers or on premises infrastructure. Furthermore, encrypting financial and customer data using proprietary keys – when properly managed –can strengthen data control and support data sovereignty.

Several non-European cloud service providers now offer sovereign cloud solutions, which may help mitigate certain geopolitical risks. However, this raises the question of whether these offerings can genuinely be considered 'sovereign.' Recently, a European taskforce proposed a 'sovereignty scoring system' that uses criteria—legal, technological, operational, economic, and cultural—to determine whether a cloud service offering can truly be considered 'sovereign'.[10] For both institutions and supervisors, these criteria may serve as a useful reference point in assessing whether sovereign cloud solutions effectively reduce dependency risks. Although the long-term viability of such solutions remains uncertain, segregating the European operations of hyperscalers can offer short-term advantages – such as gaining time to respond to data access demands from third countries. This time can be used to challenge such requests or seek alternative solutions. Ultimately, institutions must make their own strategic choices in this area. It is essential that they can clearly articulate and justify how their decisions support data sovereignty and security.

Over the longer term, it is important for Europe to become less dependent on non-European IT service providers and to achieve a greater degree of digital autonomy. Building a robust, innovative and autonomous European tech industry is advisable not only for resilience but also for safeguarding core European values such as privacy and inclusiveness. Advancing digital autonomy extends beyond the remit of individual financial institutions and national financial supervisory authorities; it requires coordinated action at the European level.

To strengthen strategic autonomy, it is necessary to reinforce the European digital infrastructure. This requires addressing the structural factors that have led to the emergence of digital dependencies. The Draghi report offers concrete recommendations to support this goal, including improving the innovation and investment climate, fostering a more dynamic business culture and removing regulatory and legislative barriers. The report highlights that Europe is rich in innovative ideas and ambition, but these are not consistently translated into commercially successful products and services. A key differentiator from the United States is the lack of an environment that actively stimulates innovation. Achieving digital autonomy hinges on the ability to support and scale innovation. According to the Draghi report, investment capital is potentially available. To mobilise this capital, the savings and investment union – supported by the AFM and DNB – plays a crucial role. In this context, access to finance with a view to scaling up innovative companies is a key focus.[11]

Reducing reliance on non-European IT service providers will require the development of fully fledged European alternatives. Where feasible, financial institutions could consider engaging with European IT vendors to support critical services. To achieve the necessary scale, institutions can collaborate on defining specifications for cloud applications, conducting joint testing – supported by auditors and IT auditors – and offering purchase guarantees. Such coordinated efforts may help accelerate the emergence of European hyperscalers. In terms of investment, collaboration among financial institutions can also help mitigate

10 Drafting European Sovereignty Criteria for Software and Digital Systems. This proposal still requires further operationalisation before it can be applied in practice.

11 For further context, see: letter from the Minister of Finance to the House of Representatives concerning the Netherlands' commitment to the Capital Markets Union.

the risk of a 'first mover disadvantage,' where early adopters may face higher costs or risks compared to those who invest later.

While strengthening Europe's tech sector is a vital step toward reducing digital dependencies, it represents only one dimension of the broader and more complex challenge of achieving digital autonomy. Addressing these dependencies requires more than simply encouraging European suppliers to expand their range of solutions. European providers do not automatically eliminate risks such as vendor lock-in or market concentration; they must also be competitive in terms of price, quality, reliability and cyber security. Without meeting these conditions, encouraging European alternatives may inadvertently lead to suboptimal choices for financial institutions – particularly in areas such as service quality and user experience.

The rise of AI also calls for targeted policy attention to mitigate concentration risks in this sector. Although dependency risks in generative AI are currently limited, the technology is evolving quickly. European AI providers are active, but structural challenges – such as an unfavourable investment climate – mirror those that have led to high dependence on non-European players in other digital domains. It is important to encourage the development of genuinely European AI alternatives. Achieving this will require coordinated efforts to reach a scale that can compete with non-European services, foster a competitive market and prevent new forms of vendor lock-in.

The AFM and DNB will examine the extent to which financial regulation (including DORA) and supervisory practice create barriers to selecting European IT suppliers or hinder innovation. Identified issues may prompt policy initiatives in the European context, engagement with legislators or adjustments to supervisory practice. This will allow institutions to consider the need for sovereignty against other characteristics when choosing their digital service provider.

Where necessary, existing regulations can be improved. EU legislation – particularly the DORA regulation – provides extensive coverage of third-party IT service risks, but certain limitations remain. While DORA addresses concentration risks and the potential impact of sanctions, there is room to reinforce these areas. Notably, ecosystem risks are not fully captured, and DORA does not impose requirements regarding the geographical location of data storage and processing – an aspect that could be reconsidered. In addition to refining existing provisions, the scope of current legislation could be expanded to include other relevant entities. The AFM and DNB will ask European supervisory authorities to evaluate whether DORA sufficiently enhances resilience to geopolitical risks and, if not, to consider issuing further guidance. The DORA oversight framework for large pan-European IT providers could serve as a foundation for more explicit and enforceable supervision. While current supervision represents a meaningful first step, the effectiveness of enforcement mechanisms will need to be demonstrated over time.

The AFM and DNB advocate for European policymakers to explore the eventual establishment of a cross-sectoral European cloud supervisor. While a comprehensive regulatory framework has emerged around specific aspects of large IT service providers' activities, the diverse operations and risks of these firms make it difficult for individual specialist regulators to effectively supervise all associated

risks. One potential solution is the creation of a centralised supervisory authority with a cross-sector mandate.[12] Such a supervisor would require a broader and more robust mandate than currently provided under the DORA oversight framework, along with greater resources. This authority could also be tasked with addressing geopolitical risks, including the enforcement of truly sovereign cloud solutions.

The AFM and DNB can strengthen their efforts by seeking cross-sector collaboration with other national authorities, such as the ACM and the RDI. By working together to promote secure, reliable and sovereign digital infrastructure, supervisors can influence market dynamics and guide technology choices. This requires a shared understanding of risks, dependencies and public interests – supported through joint working groups, policy alignment and the exchange of supervisory insights. At the same time, the pursuit of digital autonomy extends beyond national competencies. Reliance on non-Europeanl technology providers and infrastructure warrants a coordinated European approach. While national regulators can provide direction and signal priorities, meaningful progress toward digital sovereignty will depend on European-level policymaking, investment and standard-setting. A more resilient and autonomous digital future can only be achieved through cooperation within the European Union.

12 For more context, see DNB (2021) Changing landscape, changing supervision.

De Nederlandsche Bank N.V.
PO Box 98, 1000 AB Amsterdam
+31 (0) 20 524 91 11
dnb.nl/en

Follow us on:
Instagram
LinkedIn
X

Autoriteit Financiële Markten
PO Box 11723
1001 GS Amsterdam
afm.nl/en

Follow us on:
Facebook
LinkedIn
X

DeNederlandscheBank
EUROSYSTEEM

AFM