



Association Europe-Finances-Régulations

Paris, 15 October 2026

Innovation, Security and Technological Sovereignty: Reconciling Three Imperatives

Speech by Denis Beau

**First Deputy Governor of the Banque de France
and Delegated Chairman of the ACPR**

Ladies and gentlemen,

I would first like to thank the Association Europe-Finances-Régulations for its kind invitation for me to open the debates of this seminar dedicated to the digital sovereignty and operational resilience of the financial sector, which I am very happy to welcome here at the Banque de France. **The financial sector currently faces a dual imperative: expanding its range of digital services while ensuring the security of its operations.**

In order to meet both these objectives simultaneously, **the most straightforward solution is often to rely on hyperscalers**, which offer high-performance infrastructure and services – particularly in the areas of cloud computing and artificial intelligence (AI) – while providing state-of-the-art security guarantees. However, this choice leaves financial institutions **exposed to a new risk: digital dependency**. Such dependency may prove costly in the long term. A study commissioned by the association of major French companies for digital technology (CIGREF) estimates that Europeans spend EUR 264 billion each year on US software and cloud servicesⁱ. It is also operationally dangerous, as illustrated by recent discussions surrounding the possibility of a “kill switch” affecting US digital services.

This situation highlights the difficulty of the technological choices that financial actors must face today. **The challenge, therefore, is to ensure that innovation, security and sovereignty do not become competing objectives**. In this context, I would first like to examine the risks that excessive dependency could pose to the financial sector (I), before discussing the practical responses that financial institutions and public authorities can each find to address them (II).

*

I/ Security and sovereignty risks ultimately stem from the same issue: maintaining control over critical digital infrastructure. By “handing over the keys” to a few indispensable service providers over which they have little leverage, financial institutions can place themselves in a vulnerable position, for at least **three reasons**.

First, provider concentration has itself become a source of operational risk. This risk can be further amplified when institutions rely on the same cybersecurity solutions. The CrowdStrike incident in July 2024 provides a clear illustration: a defective software update caused 8.5 million computers around the world to fail simultaneously. **Next, dependence reduces institutions’ capacity to manage operational – and therefore cyber – risk.** By entrusting certain activities to third parties, **financial institutions may gradually lose the ability to carry them out themselves and, above all, to make a proper assessment of the quality of the service provided.** The loss of expertise also makes exercising effective control over IT service providers more difficult. **Lastly, by outsourcing certain critical services, institutions are exposing**

themselves to a phenomenon of “vendor lock-in”, which can manifest itself in very concrete ways through substantial cost increases once a dependency has been created, or the obligation to pay for unwanted functionalities (a practice known as **“bundling”**).

Nonetheless, despite these risks, avoiding dependencies is not easy. The case of **frontier AI models** provides a particularly illuminating example. On the one hand, it is becoming increasingly clear that these models will be an indispensable tool for cybersecurity because, while they can unfortunately provide attackers with offensive capabilities, they also offer new possibilities to security teams, both for identifying vulnerabilities and for automatically generating patches. **However, taking full advantage of these solutions often requires granting them very broad access to the institution’s information system, which in turn creates new risks:** the risk of compromise, but also the risk of transferring the financial sector’s informational capital to a few large non-European technology providers.

II/ How, then, can we balance innovation, security, and the management of the risk of technological dependence? Without claiming to cover every aspect of such a broad topic, I would like to discuss a few courses of action available to financial institutions, as well as the essential role that public authorities must play.

First, financial institutions must strengthen the way dependencies are taken into account in their operational risk assessments by conducting a systematic inventory of critical dependencies covering all their IT assets (workstations, networks, hardware, software, cloud services, security equipment, etc.). Although complex, this exercise is essential for gaining a comprehensive view of risk exposure. Benchmark indicators, such as the Digital Resilience Index (IRN), developed by a consortium of public sector entities, businesses, and digital experts, can be useful tools in this assessment.ⁱⁱ

Identifying dependencies should then enable financial institutions to develop operational resilience strategies that are consistent with maintaining control over their technological infrastructure, data, and critical digital capabilities, by implementing “multi-cloud” or “hybrid cloud” strategies for example, or by preparing exit options that ensure the portability of data and applications. The use of open-source solutions also represents a promising avenue for limiting dependencies on non-European proprietary technologies.

Of course, when faced with challenges that extend beyond the scope of any single institution, **public authorities also have a role to play.** I would like to emphasise first and foremost that, by promoting fundamental European values, **European regulations**, such as the GDPR or the AI Act, **contribute powerfully to the assertion of our sovereignty.** We should resist the temptation

to view them as obstacles to innovation, through a dangerous reversal of the hierarchy between ends and means.

However, this regulatory sovereignty must be backed by genuine technological capabilities. The “technological sovereignty package” proposed by the European Commission, which notably includes the Cloud & AI Development Act (CADA)ⁱⁱⁱ, represents a significant new step in this regard. Other, more qualified speakers will discuss this in greater detail later, but this legislation aims to facilitate the deployment of cloud computing and AI in the EU; in particular, it proposes **a single classification system** to assess the level of sovereignty of a cloud service.^{iv} The package also includes an open-source strategy aimed at **ensuring continuous access to the most critical software components**.

Beyond defining the rules, public authorities also have a vital role to play in their practical implementation. Firstly, this entails close cooperation between our various supervisory institutions, which is essential both for sharing information and for ensuring effective coordination when our areas of jurisdiction converge or even overlap. The **Banque de France and the ACPR thus renewed their cooperation agreement with ANSSI** last July^v in order to continue developing our operational synergies and adapt them to the new framework resulting from regulatory changes.

Financial authorities, for their part, can play at least two complementary roles. First, they serve as **watchdogs** through their oversight mission. The implementation of **the DORA regulation** has also led us to step up our efforts in several areas, such as digital resilience testing and the monitoring of major incidents reported by the sector. Effectively carrying out this mission requires **constant monitoring of digital risks and cyber threats**. The emergence of **frontier AI models** has therefore prompted us to develop a dedicated action plan, set out in **a communication sent by ACPR to industry associations** last June. This plan highlights two priorities: first, the implementation of fundamental cybersecurity hygiene measures; and second, the faster deployment of security patches to address the growing pace at which malicious actors are exploiting vulnerabilities.

Furthermore, by subjecting **critical third-party providers (CTPPs) to a coordinated European oversight framework**, DORA enables financial regulators to better assess risks related to concentration, dependency, and technological lock-in. Ultimately, this will enable them to better align the objectives of operational security and digital sovereignty, promote appropriate practices, and adapt their actions to rapid changes in the technological environment.

Second, we can play **a catalytic role through the technological choices we make for our own needs**, choices that are likely to influence decisions in the financial sector. In fact, the **Banque**

de France itself faces the difficult trade-offs I mentioned earlier, particularly in its roles as a central bank and as an operator of market infrastructure. To address this, it has decided to adopt a **digital sovereignty doctrine**, which directly guides our 2028 strategic roadmap and the management of our IT projects. **This doctrine can be summed up in one sentence: controlling our data, our infrastructure, and the skills needed to operate them.**

To illustrate this doctrine, let me conclude by mentioning **two ongoing projects**. First, the upcoming rollout of **Mistral AI solutions hosted on a sovereign cloud**, for daily use by our staff as well as for the protection of our information systems. And second, **the development of a virtualisation solution for our private cloud based on open-source technologies**, which should enable us to optimise our IT resources without relying on proprietary tools. In addition, we are exploring collective measures within the Eurosystem to mitigate major risks related to suppliers.

*

As you can see, I am convinced that to reconcile innovation, security and sovereignty, it is essential to ensure operational control over our digital infrastructure through a clear and coherent strategy. Recent and upcoming legislative changes are specifically designed to encourage the financial sector to fully integrate these issues into its decision-making and to broaden the range of available European solutions by fostering the emergence and development of sovereign offerings. I therefore hope that this morning's discussions will make a useful contribution to our collective reflection, and I wish you all an excellent seminar.

ⁱ CIGREF, 2025. Figures extrapolated from the expenditure data of 6 large “benchmark” companies

ⁱⁱ [aDRI - Digital Resilience Initiative](#)

ⁱⁱⁱ [Communication on European Technological Sovereignty, accompanied by an EU Open Source Strategy](#)

^{iv} [Cloud and AI Development Act | Shaping Europe's digital future](#)

^v [ANSSI, Banque de France and ACPR sign an agreement and reinforce their cooperation on cybersecurity](#)