Position paper

Transparency Register Number: 0767788931-41

Digital sovereignty and resilience in the banking sector – ensuring the ability to act in an interconnected world

- Digital sovereignty and cloud strategies
- Regulatory aspects of new technologies
- DORA review
- Regulatory coherence and regulatory relief

29.04.2026

Executive Summary

The European banking and financial sector faces complex challenges posed by technological innovation, digital connectivity and increasing regulatory requirements. Digital sovereignty, regulatory compliance, operational resilience and the capacity for innovation are now closely interlinked. This document highlights the key areas for action and provides guidance for banks, regulators and policymakers.

1. Digital sovereignty and cloud strategies

Banks must preserve their ability to act and make decisions within a globally interconnected IT landscape. Digital sovereignty does not mean autarky, nor does it imply the exclusive use of solutions and products from the EU. Rather, it refers to maintaining control over data, infrastructure, and applications—including the use of global providers—provided that autonomous and secure usage can be ensured and lock-in scenarios are avoided.

Hybrid and multi-cloud strategies, as well as modern architectures, enhance resilience and flexibility and therefore offer significant opportunities. At the same time, they are typically associated with considerable additional complexity and, not least, increased costs. The adoption of new technologies such as AI requires transparent governance, a strategic assessment of risks, and active management of dependencies.

2. Regulatory aspects of new technologies

New technologies such as AI, automation, service-oriented architectures with a focus on APIs, and cloud-native development and operating models are fundamentally transforming banking processes. Existing technology-neutral regulatory frameworks are reaching their limits of interpretation—for example, when it comes to operationalizing appropriate controls in the context of self-learning systems, or in complex multi-cloud setups with containerized, dynamically scaling workloads.

Association of German
Public Banks, VÖB, e.V.
Lennéstraße 11, 10785 Berlin, Germany
www.voeb.de

President: Thomas Groß
Vice President: Erk Westermann-Lammers
Executive Managing Director and
Executive Board Member:
Iris Bethge-Krauß

Banks require sufficiently flexible supervisory leeway that enables risk-based, proportionate, and practical implementation—without hindering innovation or competitiveness. The quality, consistency, and timing of primary and secondary legislation are crucial for feasibility and planning certainty.

3. DORA review: proportionality and practical applicability

DORA establishes a unified framework for managing ICT risks. Banks welcome this objective, but are experiencing significant effort related to documentation, third-party risk management, and reporting requirements. The principle of proportionality has not yet been sufficiently operationalized. The upcoming DORA review should enable practical adjustments, including:

- the introduction of an intermediate category for institutions that are not systemically important but still of considerable size,
- the recognition of existing security standards to avoid duplicate audits,
- the optimization of reporting processes, thresholds, and the use of the Single Entry Point.

4. Regulatory coherence and relief (cross-cutting topic)

The growing number of new and existing IT-related regulations is leading to redundant requirements and increased operational effort. Greater coherence, harmonization, and proportionate design of requirements are essential to reduce this burden, safeguard innovation cycles, and strengthen digital resilience. Differentiation based on systemic relevance enables targeted relief for institutions that are not systemically important.

1. Digital sovereignty and cloud strategies ensuring the ability to act in an interconnected world

1.1 Digital sovereignty: not autarky, but control over decisions

Resilience, independence, and digital sovereignty have become central topics in both the political discourse and the financial industry. Key drivers include unexpected geopolitical disruptions and political sanctions, which have exposed dependencies and vulnerabilities in global value chains and technology supply chains—for example through longer delivery times and price volatility. **Against this backdrop, IT-related dependencies must be reassessed from economic, technological, and security perspectives.**

For financial institutions, a key question is how to address the changing likelihood of risks associated with strategic digital dependencies. Which technological options are realistic, economically viable, and manageable in the long term? Which dependencies can be reduced or diversified, and which will inevitably remain despite significant efforts

Full digital sovereignty in the sense of technological autarky is neither achievable nor desirable. What is needed instead is a pragmatic approach based on choice, flexibility, and the conscious management of dependencies. The objective must be to strike a balance between control and the use of high-performing, competitive offerings across national, European, and global markets. Building digital resilience must not be seen as a trade-off against the ability to innovate. On the contrary, a robust

and technologically modern foundation is a prerequisite for deploying innovations in a secure, scalable, and trustworthy manner. Without an adequate level of resilience, new technologies themselves can become a competitive risk. For banks in particular, the timely adoption of new technologies is essential to efficiently meet regulatory requirements, manage operational risks, and remain competitive internationally.

In the banking context, digital sovereignty means **the ability to manage digital resources, data, and technologies autonomously, securely, and in compliance with regulations—including the use of external providers, the active management of dependencies, and the continuous preservation of decision-making and operational capability**. It is not about achieving full technological independence; in a globalized digital economy, autarky would be neither realistic nor economically viable.

True sovereignty lies in the ability to make independent technological decisions, to understand available alternatives, and to actively manage dependencies. This explicitly includes the use of global technology providers, particularly where innovation impulses are currently driven by third parties, often from the United States. Digital sovereignty is therefore not about isolation, but about consciously shaping unavoidable dependencies. It goes beyond formal control to encompass actual operational capability and self-determination over critical and differentiating assets, transparent structures, and realistic choice and exit options.

This principle of decision-making autonomy has a direct impact on cloud strategies, data control, and the use of new digital features—topics that will be explored in more detail below.

1.2 Cloud strategies as a foundation for digital operational capability

In the infrastructure domain, many banks are already well advanced today. Hybrid and multi-cloud strategies—such as combining multiple hyperscalers with in-house data centers—form the backbone of modern banking IT. The use of container and Kubernetes architectures increases application portability and enables flexible workload distribution.
These architectural approaches do not create full interchangeability between cloud providers, as specific services, tools, and analytics capabilities are often not equally substitutable. This is partly because cloud services are frequently based on proprietary technologies. In addition, extraterritorial legal frameworks (such as the US CLOUD Act and FISA 702) may apply even when data is hosted in Europe.
Nevertheless, these approaches strengthen **strategic resilience** by reducing dependencies and at least keeping exit options fundamentally available. What matters less is technical perfection, and more the fact that **decision-making authority over the infrastructure** remains with the banks—even if this comes with increasing complexity and higher demands on governance and control.

1.3 Data control as the core of bank-specific sovereignty

Banks have traditionally maintained a high degree of digital sovereignty in their handling of data. Through encryption—even in cloud environments—clearly defined access concepts, and the retention of cryptographic keys under their own control, banks preserve full control over their data at all times.
Data can be secured, moved, and analysed without structural dependence on individual providers. This data sovereignty is a central pillar of bank-specific digital sovereignty and simultaneously forms the

foundation for regulatory compliance, information security, trust, and thereby resilience. It is therefore decisive for competitiveness.

1.4 New dependencies through innovative digital features and AI

The situation is significantly more complex in higher-level digital functions—particularly AI-based services, automation solutions, and specialised development and analytics tools. In these areas, a small number of highly innovative providers—predominantly from the United States—currently dominate the market, with solutions deeply embedded into existing platforms and processes.

Such dependencies are currently difficult to avoid and have often been consciously accepted from an innovation and efficiency perspective. However, **they must be made transparent, actively managed, and strategically assessed**—including with regard to regulatory requirements, concentration risks, and long-term controllability.

For the practical use of AI-based solutions—particularly in sensitive areas such as software development, testing, or production-related processes—it may be useful to further specify existing requirements through clearer, practice-oriented minimum guardrails. These should focus on core elements such as traceability, validation, documentation, and control mechanisms. The objective is not additional detailed regulation, but a consistent interpretation that enables safe and reliable use of AI without unnecessarily restricting innovation space.

In the context of established control principles, the question also arises of how AI can be integrated into existing governance models. This is particularly relevant for the four-eyes principle. In practice, AI is already partially used in a supporting role—for example as a “first pair of eyes” in analysis, coding, or review processes. Clarification of supervisory expectations—particularly that ultimate accountability remains with humans and under which conditions AI may be used in a supporting capacity—would create additional legal certainty.

European alternatives are still largely in development; public and European funding measures are important but cannot offset the existing investment advantage of global providers in the short term.

1.5 Implications and expectations from the banking perspective

Digital sovereignty does not emerge from additional regulation, but from **frameworks** that enable autonomous technological decision-making.

A **strong and competitive ICT ecosystem** is needed to provide financial institutions—and other sectors as well—with the freedom to select the technologies and services that best suit their needs. It must be acknowledged that European providers, particularly in the Platform-as-a-Service (PaaS) and Software-as-a-Service (SaaS) segments, currently do not reach a comparable level of functionality in breadth and depth as global leading US cloud providers. Achieving full control across all ICT value chain layers is complex and requires substantial investment. However, this is not only a question of investment, but above all of building specialised expertise and robust governance structures. Through the long-term establishment of platforms that support the exchange of best practices, as well as the promotion of open standards and interoperable solutions, digital sovereignty can be effectively strengthened. In this

way, Europe can assume a pioneering role in digital sovereignty while simultaneously promoting choice and competitiveness for institutions. In particular, institutions—and other industries as well—can strengthen their independence through local solutions and partnerships with European providers and ensure compliance with local data protection requirements. A fully comprehensive cloud sovereignty across all dimensions is, in globally interconnected IT ecosystems, practically unattainable.

A more effective approach is to define an institution-specific ambition level for digital sovereignty—differentiated across dimensions such as data control, operational manageability, architectural portability, and contractual transparency. Sovereignty is thus a strategic design task rather than an absolute state. As part of this framework, incentives should be created jointly at European state and industry level to support innovation and investment in emerging technologies. For example, super-depreciation schemes, tax incentives, and similar measures could be considered. Public funding programmes can also help intensify research and development initiatives and strengthen collaboration between companies and universities. Promoting practical cooperation between academia and industry can further expand technical expertise and enable the development of tailored solutions for the specific needs of the financial sector.

Existing regulatory frameworks are **predominantly technology-neutral and risk-based**. However, it is crucial that their interpretation and application remain practical and that legitimate requirements for controllability do not implicitly evolve into expectations of full technological autarky or unlimited substitutability. One example would be purely European certification schemes that do not reflect operational reality.

Equally important is a **coordinated European interpretation and supervisory practice** that does not restrict choice and innovation through diverging national expectations. Digital sovereignty requires that banks remain able to use global technologies responsibly, as long as controllability, transparency, and risk management are ensured.

In addition, a **clear alignment between regulation, innovation policy, and location strategy** is necessary. The development of European alternatives should be actively supported without restricting the use of existing international solutions. Banks must remain capable of adopting innovations early in order to remain competitive internationally—particularly in light of geopolitical tensions and strategic dependencies.

Finally, digital sovereignty is also a **governance responsibility of the institutions themselves**. It requires clear accountability structures, transparency regarding dependencies, and realistic exit and substitution strategies that are regularly reviewed and further developed.

Our policy asks to strengthen digital sovereignty in the banking sector

1. No implicit expectation of technological autarky in regulation
Legislators and supervisory authorities should explicitly clarify in the interpretation and application of regulatory requirements—particularly in discussions on concentration risk, exit strategies, and multi-vendor requirements—that the objective of regulation is the manageability of risks, not full technological substitutability or European self-sufficiency.

2. Technology-neutral and risk-based application of existing rules
The risk-based application of existing regulatory frameworks should be consistently aligned in supervisory practice with actual criticality and specific risk profiles.

3. Ensure a harmonised European supervisory approach
Diverging national interpretations of regulatory requirements should be avoided. Banks need consistent expectations across Europe, particularly regarding cloud usage, third-party risk management, and exit strategies.

4. "Regulate when needed" – regulation only where there is demonstrated necessity
New regulatory requirements should only be introduced where a concrete and proven regulatory or supervisory gap exists—not in a preventive manner at the expense of innovation and competitiveness.

5. Recognition of digital sovereignty as a multidimensional, risk-based target model
Digital sovereignty manifests across different dimensions—such as data access, governance structures, operational controllability, and exit options. Regulatory concepts should recognise that institutions may define and implement an appropriate level of sovereignty depending on their business model and risk profile. Full technological decoupling is not a regulatory requirement; what matters is the controllable and responsibly managed design of dependencies.

6. Promotion of open standards and interoperability instead of bespoke certification schemes
Political and regulatory initiatives should focus on internationally compatible standards, interoperability, and technical portability. Additional, non-harmonised certification requirements increase complexity and cost without necessarily delivering proportional security benefits.

7. Targeted innovation and investment incentives instead of additional compliance burdens
The development of European technological capabilities should primarily be driven through tax incentives, super-depreciation schemes, funding programmes, and R&D collaborations—not through regulatory barriers to adoption.

8. Practical recognition of geopolitical realities
Regulatory requirements should acknowledge that global dependencies cannot be fully eliminated in the short term. Banks must retain sufficient flexibility to manage risks strategically and mitigate them through diversification, contractual adjustments, or technical measures. Existing risk inventories already provide a suitable foundation for this.

9. Recognition of institution-specific governance instead of prescriptive detail rules
Supervisors and legislators should rely more strongly on internal governance, risk, and control capabilities of institutions, rather than replacing them with granular reporting and evidence requirements.

2. Regulatory aspects of new technologie
Enabling innovation within existing regulatory frameworks

2.1 New technologies within an existing regulatory framework

Regulatory frameworks in the banking sector have traditionally been designed in a technology-neutral manner. However, they were conceived in an environment where cloud-based development and operating models, AI-driven decision-making systems, or highly automated development processes were not yet dominant. In practice, this creates areas of tension between IT transformation driven by innovation and risk-based supervisory approaches. At the same time, with horizontal digital regimes such as the AI Act, a paradigm shift towards technology-specific regulation is emerging. Function-based supervision and technology-specific requirements are therefore increasingly overlapping.

For banks, new technologies do not operate in a regulatory vacuum but must be integrated into existing supervisory frameworks—particularly requirements related to governance and internal control systems (e.g. MaRisk), ICT risk management (DORA), outsourcing and third-party risk management (MaRisk AT 9, DORA Chapter V), information security (DORA), as well as data protection and compliance obligations (GDPR, banking secrecy requirements).

In practical application, however, these frameworks increasingly show interpretational and implementation limits when highly dynamic technologies such as cloud-native architectures, AI-based systems, or modular platform ecosystems are deployed. Requirements related to full transparency, continuous controllability, detailed ex-ante documentation, and formal audit rights can only be met to a limited extent in the context of learning systems, globally distributed cloud services, or deeply integrated standard platforms—without significantly impairing innovation, speed, and scalability.

The regulatory need for action therefore lies less in introducing new rules than in a **risk-based, technology-neutral, and proportionate interpretation of existing requirements** that enables innovation while safeguarding controllability and security within institutions. This also includes recognising institution-specific governance and control frameworks, as well as moving away from implicit expectations of full technical control or substitutability of every individual technology component.

2.2 AI and automation: risk, control, and accountability considerations

The use of AI-based systems and extensive automation presents specific regulatory challenges. Banks are therefore already required by legislators and supervisors to establish **appropriate governance, validation, and monitoring mechanisms**, without effectively slowing down innovation through excessive caution. Existing requirements related to model risk, internal controls, the traceability of decisions, and accountability are fundamentally applicable, but cannot always be transferred directly to learning and adaptive systems.

For banks, this creates a tension. In practice, this tension is already addressed through established governance mechanisms—such as human-in-the-loop approaches, model validation, and continuous monitoring. At the same time, the use of complex and partially pre-trained models changes the

requirements for transparency, allocation of responsibility, and depth of control. This calls for a further evolution of the supervisory perspective.

2.3 APIs, modular IT landscapes, and new dependencies

Service-oriented architectures with a focus on APIs, as well as modular, cloud-centric IT landscapes, are key enablers of innovation, collaboration, and scalability. They allow banks to integrate new services quickly, connect partners, and incrementally evolve existing systems. From a regulatory perspective, particularly relevant aspects include outsourcing, third-party risk management, and information security.

Existing regulatory frameworks—such as those on outsourcing and ICT risk—are fundamentally applicable, but only partially capture the **granularity and dynamics** of modern API services and modular IT landscapes. In highly heterogeneous and modular environments, distinguishing between internal services, external sourcing, technical interfaces, and critical services is particularly challenging. In practice, formal requirements—such as classification rules for the above-mentioned services—may lead to blanket assessments that do not fully reflect the actual risk structure of such environments.

As already outlined in section 2.1, the challenge lies less in the absence of regulation than in its application to highly modular and dynamic architectures. A more appropriate approach is to **anchor assessment in the actual risk profile of the respective function—such as criticality, data dependency, substitutability, and effective controllability—rather than in the underlying technology itself**. This would better reflect the granularity of heterogeneous and modular IT landscapes and enable the flexible use of innovative architectures. Legislators and supervisors should clarify this accordingly. Alternatively, a unified framework for ICT and non-ICT services could also be considered to improve transparency and controllability.

2.4 Technology neutrality requires interpretative flexibility

A central principle of financial market regulation is technology neutrality, which remains both valid and necessary in the context of new technologies. However, in practical implementation, it requires sufficient interpretative flexibility—for both institutions and supervisory authorities. This is particularly evident in the application of existing requirements to modular IT architectures or the use of cloud and AI systems, where requirements for documentation, accountability, and controllability cannot be defined in a one-size-fits-all manner but must depend on the individual risk profile of the institution. Instead of detailed technology-specific rules, banks require a **framework that enables risk-based, proportionate, and innovation-friendly solutions**. The key factor is not the specific technology used, but its criticality and its embedding within the overall architecture. An overly rigid or formalistic application of existing rules would otherwise unnecessarily delay or even prevent the adoption of new technologies.

2.5 Quality and timing of regulatory requirements (primary and secondary legislation)

Beyond the substantive design of regulatory requirements, **the quality and timing of primary and secondary legislation** are of central importance. For banks, it is not the volume of regulation that matters, but rather its clarity, consistency, and practical applicability within the relevant risk context.

At the level of **primary legislation**, there is a need for fewer but clearer, more precise, and more concrete requirements that enable targeted implementation. This includes clearly defined objectives, explicit expectations, and a transparent description of the mandate for delegated acts. It is also essential that the **applicable implementation period for market participants is defined only once the delegated acts have been finalised**. Implementation timelines should only begin after the finalisation of the relevant Level 2 measures.

The currently common approach—defining implementation deadlines while delegated acts are still being developed—effectively shortens the available implementation period for institutions. In practice, the final approval of delegated acts by European supervisory authorities and the European Commission is sometimes significantly delayed compared to their technical completion. Additional delays arise when changes are introduced at later stages. These uncertainties significantly complicate structured and efficient implementation.

At the level of **secondary legislation**, timely and mandate-compliant finalisation of all necessary rules is essential. Entry into force should be consistently linked to the full finalisation and formal adoption of the respective legal act—for example, publication in the Official Journal of the European Union. Only from that point should the implementation period for the market begin.

Such an approach would significantly improve predictability, legal certainty, and implementation quality—benefiting both institutions and supervisors.

2.6 Implications and expectations from the banking perspective

Against the backdrop of increasing geopolitical tensions and global technology dependencies, banks assume that new technologies can be used within the existing regulatory framework. The key requirement is that risks are appropriately managed, without innovation or competitiveness being disproportionately constrained by excessive formalisation or overly narrow interpretations of existing rules.

Technology neutrality must be given practical effect through sufficient interpretative and supervisory discretion—guided by the actual risk profile, criticality, and embedding of new technologies within the overall architecture of an institution. **Regulatory practice must not become an innovation barrier; instead, it should actively support innovation—for example through regulatory sandboxes. Other forms of flexibility are also conceivable, such as pilot schemes under simplified regulatory conditions or the recognition of agile internal governance structures for faster decision-making.**

A fundamental prerequisite **is trust in the professional and organisational capabilities of institutions to use new technologies responsibly**, in a risk-oriented and compliant manner. Banks have established governance, control, and risk management frameworks, as well as deep technical expertise, to appropriately assess and manage technological risks.

An effective regulatory framework should **leverage and strengthen these capabilities** rather than replacing them with excessive detail requirements or formalised documentation obligations. The objective is a framework that enables innovation, preserves economic viability, and at the same time

ensures controllability and safety—thereby strengthening the **long-term competitiveness of the European banking sector**.

Concretely, this means: avoiding excessive detail in delegated acts, increasing the use of risk-based supervisory discretion, and consistently recognising existing governance, control, and security frameworks within institutions. In addition, reporting obligations should focus more strongly on material risks, and duplicate assessments should be systematically avoided. Only then can a regulatory framework emerge that enables innovation while maintaining economic viability, controllability, and safety.

Our policy asks to strengthen innovation within existing frameworks

1. Risk-based assessment of AI systems
Learning and adaptive systems should be assessed primarily based on their actual risk and criticality. Requirements related to explainability and transparency should be applied by supervisors in a risk-based manner.

2. Focus on operational controllability rather than technical completeness
Formal requirements should not generically demand that every individual technical component must be fully substitutable at all times. The decisive factor is effective operational controllability within the respective risk context. For critical functions or those relevant to business continuity management (BCM), appropriately higher requirements should apply, reflecting the respective protection needs and recovery objectives.

3. Timely implementation of delegated acts
Implementation timelines should only begin after the finalisation and publication of the respective legal act, ensuring legal certainty and realistic planning horizons.

4. Avoiding innovation barriers through formalism
Regulatory reviews should be designed in a way that does not hinder the adoption of new technologies through disproportionate formal requirements.

5. Recognition of institution-specific validation and monitoring frameworks
Where an institution has established effective validation and monitoring processes for AI or automation solutions, these should be recognised in supervisory assessments. The key criterion should be whether existing frameworks adequately address the relevant risk profile—not whether they conform to a generic standard format. Redundant or purely formal parallel assessments without additional risk value should be avoided.

6. Transparent distinction between internal services, outsourcing, and critical functions
Requirements should reflect the practical reality of modular and heterogeneous IT architectures. The key is a consistent, transparent, and risk-based classification approach that enables institutions to appropriately distinguish between internal services, outsourced services, and critical functions.

7. Technology-neutral drafting of delegated acts
Regulatory requirements should remain technology-neutral. The decisive factor should be the risk profile of the application, not the underlying technology.

8. Focus on established governance, control, and risk management frameworks
Excessive detail requirements in (delegated) acts should be avoided, with greater reliance placed on risk‑based supervisory discretion. In addition, reporting and documentation obligations should focus on material risks and duplicate assessments should be systematically avoided.

3. DORA Review
Effectiveness through proportionality and practical applicability

3.1 Scope, proportionality, and reporting

The Digital Operational Resilience Act (DORA) establishes a unified European framework for managing ICT risks, which is broadly supported by banks. While its wide scope is intended to ensure comprehensive resilience of the financial system, it also creates significant challenges in practical implementation. Although the principle of proportionality is explicitly embedded in the regulation, it has so far been insufficiently reflected in the detailed design of the Regulatory Technical Standards (RTS).

From the banking sector's perspective, there is therefore **a clear need for stronger differentiation of DORA requirements**. In addition to the full application of DORA and the simplified ICT risk management framework already, a "middle tier" is missing—one that better reflects the reality of many institutions. Such differentiation, based on systemic relevance or criticality, could be applied to aspects such as the depth of documentation, scope of reporting, testing frequency, and reporting timelines, thereby operationalising the principle of proportionality more effectively.

An **appropriate reference point** for this intermediate category could be the already established supervisory risk differentiation within the Supervisory Review and Evaluation Process (SREP). Institutions supervised by BaFin are already assessed under SREP based on size, complexity, business model, and risk profile—without being formally assigned to rigid categories. DORA should build on this logic and introduce a middle-tier approach for institutions that are not systemically important but are nevertheless subject to heightened, non-systemic supervision due to their balance sheet size, operational relevance, or ICT dependencies. This would enable larger, non-systemically important institutions—such as promotional banks or large regional banks—**to implement documentation, testing, and reporting requirements in a proportionate manner without diluting the objectives of DORA**.

For this intermediate application level, reduced requirements could apply with regard to documentation depth, audit cycles, and contractual detail. For significant but not critical or important ICT third-party services, **standardised evidence** (e.g. recognised certifications) should be sufficient; additional institution-specific audits should only be required where there are **concrete indications of risk**, rather than on a routine basis. The assessment of concentration and dependency risks should focus more on the criticality of the service for the supported processes, rather than on the formal completeness of all supply chains. Supervisory expectations should be aligned with the actual risk profile and build on the differentiation already established under SREP based on size, complexity, and business model.

A **currently discussed extension of the small-institution or proportionality regime** could allow for the application of simplified requirements for smaller or less complex institutions. This would make it possible to reduce a large share of medium or non-critical ICT third-party services to standardised evidence and risk-appropriate assessments—without the need for a complex, highly granular tiering structure.

In practice, the **scope of required documentation and reporting represents** a significant operational burden, particularly for stable and well-established processes—for example, the description of cryptographic procedures, detailed testing concepts, or process documentation. This effort is often disproportionate to the additional insights gained for actual resilience. Under existing German regulation (MaRisk AT 9 para. 7 and BT 2.1), institutions are already required to include outsourced activities in their audit planning; substitute audits (e.g. conducted by Big Four firms) are permissible. Against this background, it is appropriate to design the depth of documentation and scope of audits for stable, established processes in a risk-based and event-driven manner, without compromising resilience. A lack of documentation, by contrast, would make operations and incident resolution dependent on ad hoc actions rather than structured and reliable processes.

In addition, it should be assessed to what extent documentation for less critical or stable applications can be prepared or updated more on a needs-based basis. Partial "on-demand" generation—for example in the context of audits or specific triggers—as well as bundled, periodic updates (e.g. monthly or quarterly), could significantly reduce ongoing maintenance efforts without materially limiting traceability or auditability.

Overall, it becomes evident that the RTS contain very detailed requirements regarding documentation and evidence. However, in practice, the **complex interdependencies of modern ICT systems cannot be fully captured or consistently assessed**. As a result, the effort incurred is driven less by the identification of material risks and more by granular asset, risk, and evidence management aimed primarily at fulfilling formal requirements—without adequately reflecting actual dependencies.

3.2 Third-party risk management

With DORA, the management of ICT third-party risk is significantly expanded and harmonised across Europe. The objective is to limit concentration risks, increase transparency, and strengthen the digital operational resilience of the financial system as a whole. Banks explicitly support this approach. However, in practical implementation, it becomes evident that requirements—particularly regarding contractual arrangements, audit rights, and ongoing monitoring—are associated with considerable operational and economic challenges.

A key challenge lies in the **design and enforceability of audit and access rights vis-à-vis ICT third-party service providers**. Especially when dealing with dominant market providers, institutions regularly encounter practical limits to their negotiating power. This is particularly true for complex supply chains and subcontracting arrangements, where transparency and the ability to exert influence naturally diminish. The regulatory expectation of comprehensive responsibility, including for sub-service providers, is in practice only achievable with significant effort and is not always proportionate to the level of risk that can realistically be controlled.

Against this backdrop, the adjustment introduced by the European Commission in relation to the RTS on subcontracting—**limiting audit requirements to sub-service providers that support critical or important functions**—is explicitly welcomed.

.

Requirements for fully consolidated, written contractual documentation also pose significant challenges for many institutions. Certain provisions of Article 30 DORA are particularly demanding in practice. For example, Article 30(2)(i) DORA requires agreements on the participation of ICT third-party service providers—or their staff—in the institution's **training programmes**, unless the provider already has an adequate training and awareness framework in place. Especially with international or standardised providers, such bespoke contractual arrangements are often difficult to enforce in practice.
In addition, there are **currently no standardised model clauses or supervisory-agreed contractual building blocks available**. This results in a multitude of individual contractual solutions, increased legal and organisational coordination efforts, and a fragmented implementation landscape.

In practice, it can also be observed that some providers incorporate DORA-related regulatory requirements into their pricing or charge separately for them. Particularly for market-dominant or hard-to-substitute services, institutions often have limited negotiating power. This creates a risk that regulatory requirements lead to increased costs without a commensurate improvement in resilience.

Many DORA requirements overlap with established information security and control standards. Existing certifications such as ISO 27001, BSI IT-Grundschutz, or TISAX should therefore **be explicitly recognised as suitable evidence for certain aspects of DORA compliance**—for example in relation to governance, control frameworks, or continuous improvement processes. Such recognition would avoid duplicate audits, enhance comparability, and make implementation more efficient.

At the same time, not all DORA-specific requirements can be covered by existing standards. A clear delineation is therefore necessary to ensure that additional evidence requirements focus specifically on genuinely DORA-specific aspects. Against this backdrop, a three-tier recognition and audit framework for ICT third-party service providers appears appropriate:

1. **Critical ICT third-party providers (CTPPs)**
   For CTPPs, a supervisory-aligned authorisation or recognition regime should apply, confirming through formal certification that these providers have been comprehensively assessed and that their services are regulatorily accepted. Audit results should be made centrally available to supervised institutions in order to avoid duplicate audits and redundant information requests.
2. **Providers of critical services**
   Where providers deliver critical services to an institution without being classified as CTPPs, a risk-based monitoring approach should apply. Standardised DORA evidence or recognised certifications may serve as a baseline; additional institution-specific audits should only be required where there are concrete indications of risk or an elevated risk profile.
3. **Non-critical or standardised services**
   For non-critical, standardised services—such as office software or commonly used cloud tools—significantly simplified contractual requirements and reduced documentation obligations should apply. The scope of evidence should be proportionate to the actual risk profile.

Audits could be conducted through certified, independent third-party audits with regularly rotating auditors over multi-year cycles. Audit methodologies and scope should be developed in close

coordination between supervisors and the financial industry. For market-dominant providers, a stronger role for centralised or state-coordinated audit mechanisms could also be considered in the longer term to ensure efficient and consistent supervision.

With regard to the **central register of information**, there is general support for its underlying objective. However, it is evident that the currently envisaged level of detail does not, in all areas, provide proportional added value for risk management. A stronger focus on genuinely risk-relevant information would improve data quality while reducing administrative burden. Contracts relating to non-critical or merely supporting functions should therefore be eligible for documentation in a simplified form.

In light of a potential future extension of the register to include both ICT and non-ICT functions, it is also important to take into account the different internal organisational and governance models of institutions. Whether a register is structured on a contract-based, function-based, or hybrid basis should be left to the institution. What matters is not the chosen structure itself, but a coherent overall design, consistent methodology, and clear, uniform terminology.

3.3 Incident reporting

With DORA, the reporting of ICT-related incidents is being harmonised and significantly expanded across Europe. The objective is to ensure early transparency of major incidents and to improve the exchange of information between supervisors and market participants. Banks explicitly support this objective. However, in practical implementation, it becomes evident that the current design and application of reporting requirements create operational challenges and do not always fully realise the intended added value.
From the perspective of institutions, the **thresholds for reportable incidents** appear in part to be set relatively low; in addition, certain reporting criteria require further clarification in practical application.

Data availability plays a central role within the DORA reporting framework. It is both a component of the “data loss” criterion and indirectly relevant for the duration of service disruptions and the criticality of affected functions. In practice, this can lead to situations where multiple reporting criteria are triggered simultaneously at an early stage of an incident—even where the issue is an internal, operationally manageable disruption without external impact. The lack of a clear distinction between technical impairment and supervisory relevance encourages precautionary reporting and increases resource requirements, without a corresponding increase in informational value for supervisors.

The **criterion of customer impact** also proves challenging. At the early stages of an incident, it is typically not possible to reliably assess how many customers will actually be affected or what the implications for reputation and market behaviour may be. Reputational damage can rarely be determined with certainty within the prescribed timelines, unless a cyber incident becomes publicly known. As a result, this criterion is often assessed on a precautionary basis, meaning that an incident—particularly in combination with a potential data loss—is classified as major at an early stage, even if this assessment is later revised.

In addition, the existing criteria do not fully capture all relevant impacts in a sufficiently differentiated manner. **Internal effects** on critical processes, control functions, or the institution as a whole may be significant without immediately being reflected in customer numbers or transaction volumes.

Against this background**, a more differentiated approach based on the type and risk relevance of an ICT-related incident** appears appropriate. The decisive factor should not be limited to the immediate impact, but should also consider whether there is a (foreseeable) breach of institution-specific recovery objectives (RTO/RPO). Internal disruptions that can be resolved within these targets and do not stem from security-related causes typically do not pose an elevated resilience risk. A classification more closely aligned with these parameters would better reflect the institution-specific risk profile and risk appetite. By contrast, a purely impact-based approach is insufficient and may lead to disproportionate reporting efforts without generating additional supervisory insight.

In operational practice, it is also evident that, particularly in the early stages of an incident, it is often not possible to clearly determine whether reporting thresholds have been met. This results in increased coordination, training, and alignment efforts and encourages a precautionary reporting approach.

Another challenge is the requirement for **unrestricted reporting obligations over weekends and public holidays**. Unlike previous frameworks, no relief mechanisms are предусмотред. In practice, it is often difficult to gather all the information required for a qualified report within a short timeframe during weekends, as specialised staff are not always fully available. This can lead to reporting under significant time pressure while simultaneously diverting resources from incident resolution. A more differentiated and practice-oriented design of reporting timelines—potentially with stronger alignment to existing regimes—could improve reporting quality.

Further burdens arise from the **design of reporting processes and templates**. The repeated submission of identical information across initial, intermediate, and final reports, the absence of pre-filled master data, and technical barriers contribute to increased administrative effort. This effort is not always proportionate to the additional insights gained.

On a positive note, DORA as a *lex specialis* has the potential to contribute to the consolidation of reporting through a central reporting hub. Germany already provides an example with its centralised reporting to BaFin. The **Single Entry Point** envisaged under the Digital Omnibus could—particularly for sectors that are not yet familiar with such centralisation—offer an opportunity to streamline reporting obligations, avoid duplicate submissions, and ensure consistent outputs in urgent situations.
From the perspective of institutions, such a Single Entry Point should, however, take into account the practical experience gained from DORA implementation at an early stage. While the overall number of reports has not increased significantly—existing notifications are often now channelled through DORA—the **effort per report** has increased noticeably. This is particularly due to complex pre-assessment requirements and detailed formal specifications, without always delivering a corresponding increase in value.

A key prerequisite for an effective Single Entry Point is its consistent design as an instrument for **harmonising and simplifying existing requirements**. Real added value will only be achieved if reporting concepts, incident categories, severity levels, and thresholds are aligned in a coherent and consistent manner. The Single Entry Point should not merely function as a technical aggregation platform, but should go hand in hand with a reduction of redundant reporting fields, clear criteria, and simplified processes—particularly with a view to potential future reporting regimes under frameworks such as the AI Act or the Cyber Resilience Act.

3.4 Implications and expectations from the banking perspective

DORA establishes a unified European framework for managing ICT risks and is broadly welcomed by banks. However, its implementation shows that the highly detailed scope of application and extensive reporting obligations lead to significant operational effort in practice—particularly in the areas of documentation, third-party risk management, and incident reporting. The principle of proportionality has so far not been sufficiently operationalised, with medium-sized institutions being particularly affected by the current requirements.

The upcoming **DORA review** should therefore ensure that requirements are designed in a practical, proportionate, and manageable way. Key aspects include:

- the introduction of an intermediate category for institutions that are not systemically important but are large and complex, enabling a reduced and proportionate application of DORA requirements,
- the recognition of existing information security standards as evidence for parts of DORA compliance, in order to avoid duplicate audits,
- the adjustment of reporting processes, thresholds, and criteria, in particular: differentiation by root cause, avoidance of unnecessary weekend reporting, and the use of the Single Entry Point as an effective instrument for simplification.

In addition, the DORA review should take into account the **broader regulatory context**: harmonisation, coherence, and a reduction of the operational burden on banks are essential to strengthen innovation, competitiveness, and digital resilience in a geopolitically sensitive environment. Only in this way can banks maintain their ability to act, effectively manage risks, and leverage technological opportunities.

Our policy asks for a practical and proportionate application of DORA

1. Introduction of an intermediate requirement category

Institutions that are not systemically important but are large and complex should be able to comply with DORA requirements in a reduced and proportionate manner (e.g. documentation, testing frequency, reporting obligations).

2. Recognition of existing information security standards for the intermediate category

Standards such as ISO 27001, BSI IT-Grundschutz, or TISAX should be recognised as evidence for parts of DORA compliance, in order to avoid duplicate audits.

3. Risk-based and differentiated documentation requirements

Reduce the level of detail for stable, well-established processes and focus on risk-relevant information rather than the full documentation of entire supply chains.

4. Central Single Entry Point

Use it as a tool for streamlining, harmonising, and standardising reporting; reduce redundant data fields and define clear, consistent criteria.

5. Differentiation in incident reporting

Establish a clear ex-ante distinction between internal operational disruptions and external security incidents; introduce higher thresholds or explicit exemptions for internal incidents that can be resolved within defined RTO/RPO targets.

6. Flexible weekend and public holiday reporting

Align reporting obligations with the institution's risk profile and harmonise them with other reporting regimes (e.g. GDPR), allowing for more practical implementation.

7. No blanket audit requirements—particularly for dominant providers

Avoid generic or event-independent audit requirements where standardised, recognised evidence is available and no specific risk indicators exist.

8. Standardised contractual clauses for third-party providers

Provide supervisory-agreed model clauses to reduce legal complexity and coordination effort.

9. No mandate overreach in Level 2 measures – effective application of proportionality

Ensure that delegated acts do not exceed their mandate and that proportionality is effectively applied in practice, particularly regarding documentation depth, testing cycles, and reporting requirements based on size, complexity, criticality, and SREP differentiation.

10. Three-tier recognition and audit framework for ICT third-party providers

Critical ICT third-party providers (CTPPs): Formal recognition confirming that providers have been comprehensively assessed and their services are regulatorily accepted.
Providers of critical services: Standardised DORA evidence or recognised certifications as a baseline; additional institution-specific audits only where concrete risk indicators or elevated risk profiles exist.
Non-critical or standardised services: Significantly simplified contractual requirements and reduced documentation obligations; the scope of evidence should be proportionate to the actual risk level.

4. Regulatory coherence and relief

Outlook

The growing number of new and existing IT-related regulations—from DORA to the Cyber Resilience Act (CRA), NIS2, and various sector-specific requirements—leads in practice to complex and, in some cases, redundant obligations for banks. A comprehensive review of all relevant primary and secondary legislation with regard to necessity, practical applicability, and supervisory effectiveness is therefore urgently needed. Overlapping requirements should be identified, non-essential elements eliminated, and the remaining obligations clearly aligned with a cost-benefit perspective—ideally through a bundled omnibus approach.

Particular attention should be given to differentiation based on systemic relevance: while systemically important institutions are subject to comprehensive requirements, non-systemically important institutions should benefit from meaningful relief. This strengthens proportional implementation and reduces operational burden without compromising the stability of the financial system.

Regulatory coherence is also closely linked to innovation capacity and geopolitical challenges. Banks must be able to adopt new technologies—such as AI, cloud solutions, or digital platforms—without unnecessary regulatory complexity hindering innovation cycles. At the same time, they must manage dependencies on international technology providers and make strategic decisions in a sovereign manner.

Efficient, coherent, and proportionate regulation is therefore a key lever to strengthen digital resilience, innovation capacity, and competitiveness. It enables banks to leverage technological opportunities, effectively manage operational risks, and avoid unnecessary administrative burden.

Overall conclusion

Banks can only operate successfully, resiliently, and in an innovation-friendly manner if digital sovereignty, technological innovation, DORA-compliant ICT risk management, and regulatory coherence are effectively interlinked. An isolated view of individual regulatory frameworks falls short: only an integrated approach that combines self-responsibility, practical applicability, and proportionate effort can create a solid foundation for resilient and competitive financial institutions.

The key areas of action can be summarised as follows:

- **Digital sovereignty:** Decision-making authority over data, infrastructure, and applications—including the use of global providers—is central to flexibility and innovation capability. **Within their existing risk frameworks and governance systems**, banks can implement this approach in a way that enables the safe use of new technologies such as hybrid multi-cloud architectures or AI solutions within the current regulatory perimeter.
- **Practical regulation of new technologies:** Technology-neutral frameworks must be interpreted in a flexible, risk-based, and proportionate manner in order to adequately govern modular, hybrid, and API-driven IT landscapes. Overly rigid and formalistic requirements risk constraining innovation and increasing operational risk.
- **DORA implementation:** The unified European framework for ICT risk is broadly supported by banks but requires practical operationalisation. Key elements include the introduction of an intermediate requirement category, recognition of established security standards, proportionate documentation and reporting obligations, and the effective use of a Single Entry Point.

- **Third-party risk management:** Risk-based assessments of critical and important services, standardised contractual building blocks, and the avoidance of blanket audit obligations are essential to reduce complexity, improve controllability, and ensure resilience in complex supply chains.
- **Incident reporting:** Differentiated thresholds, a clear distinction between internal operational disruptions and external security incidents, and practical reporting timelines—particularly during weekends and public holidays—are necessary to ensure efficient, risk-based reporting without unnecessary administrative burden.
- **Regulatory coherence and relief:** Harmonisation and the reduction of redundant requirements are key to lowering operational burden, enabling innovation, and strengthening digital resilience. Differentiation based on systemic relevance ensures proportionality and targeted relief for non-systemically important institutions.
- **European simplification and harmonisation:** Current EU efforts to review, harmonise, and simplify regulatory requirements—such as the Digital Fitness Check—offer an important opportunity to reduce duplication, inconsistent requirements, and unnecessary complexity. These principles of simplification, harmonisation, and practical operationalisation can be effectively applied to DORA and related regulatory frameworks. From a banking perspective, this means that established standards, risk-based assessments, and proportionate reporting processes can be consistently leveraged to reduce administrative burden while fully meeting regulatory objectives.

In summary, only through the consistent integration of **digital sovereignty, technological innovation capability, practical DORA implementation, and regulatory coherence**—complemented by the opportunities of European simplification and harmonisation—can banks effectively manage risks, harness the potential of new technologies, and safeguard their operational resilience. This holistic understanding forms the basis for a future-proof, resilient, and competitive European financial system, particularly in light of ongoing geopolitical uncertainty.