BAFIN IMPLEMENTATION GUIDELINES ON DORA

SUMMARY INFORMATION PACK

September 2024

REPLY

Executive Summary

On 19 September 2024, Germany's Federal Financial Supervisory Authority (BaFin) published a supervisory statement [1] covering its guidance on the implementation of the Digital Operational Resilience Act (DORA). Primarily aimed at banks in-scope of both the BaFin's BAIT/VAIT IT requirements and the DORA's information and communication technology (ICT) risk rules, the guidance also applies to institutions with similar IT supervisory expectations, such as asset managers, payments, and electronic money firms.

The BaFin intends to achieve three primary objectives with the supervisory statement:

Support in-scope firms to map and implement DORA's ICT risk and third-party risk requirements

Identify key areas of regulatory divergence where the DORA goes beyond the BaFin's requirements

Scope the desired outcomes emerging from DORA and its regulatory technical standards

This information pack summarises the BaFin's key findings on regulatory divergence to support in-scope firms with identifying the emerging outputs, across policies, frameworks, and capabilities, to be developed to embed the guidance. The supervisory statement discusses DORA under eight key themes:

1. **Governance and Organisation**
   DORA's requirement for an ICT risk and ICT third-party risk-driven digital resilience strategy and the expanded oversight role of the management body
2. **Information Risk and Information Security Management**
   The focus on ICT risk management over traditional security, heightened control requirements, and training obligations
3. **IT Operations**
   Requirements for operational stability and resilience of ICT systems, comprehensive change management, and enhanced data integrity
4. **ICT Business Continuity Management**
   Embedding a robust ICT business continuity policy, testing capabilities, and the role of a crisis management function
5. **ICT Project Management and Application Development**
   ICT project and change management, and expectations on system acquisition, development, and maintenance
6. **ICT Third-Party Risk Management**
   Concept of ICT third-party risk management, widening scope of contractual requirements, and exit strategies for critical functions
7. **Operational Information Security**
   Stronger network security measures and rigorous data encryption standards for protecting data in use
8. **Identity and Access Management**
   Identity management expectations and the expansion of access control architecture with the "need to use" principle and additional enhancements

1. Guidance notes on the implementation of DORA for ICT risk management and ICT third-party risk management, BaFin (2024)

Overview of Guidance Notes on Implementation (1/2)

Theme	BaFin Identified Areas of Regulatory Divergence	Key Outputs Expected from In-Scope Firms [2]		
Governance and Organisation 	DORA's strategy requirements focuses on ICT risk and third-parties whilst the BaFin is cross-cutting across overall IT capabilities BaFin's expectations on management body oversight is less extensive than DORA's requirements Clear requirement under DORA for the management body to be aware and upskill on ICT risk, with no explicit equivalent under BaFin	Digital Resilience Strategy An ICT risk and third-parties focussed digital resilience strategy	Management Body Oversight Evidence of oversight role (e.g. updated terms of reference and meeting notes)	Training and Awareness Comprehensive ICT risk training strategy for the management body
Information Risk and Information Security Management 	DORA has a strong focus on ICT risk management against BaFin's more traditional focus on operational risk and information security Greater focus on firm-wide ICT security awareness and incident communications in DORA	ICT Security Awareness ICT security awareness plan for the whole firm and management body	Incident Communications Clear communication plans for major incidents, with clear responsibilities	Internal Control Established control policies to analyse new assets, legacy tools, incidents, and testing outcomes
IT Operations 	Operational stability an expanded priority under DORA, covering ICT testing, capacity management, and processing power during stress BaFin has lighter requirements on data integrity checks and reconciliations compared to DORA	ICT Testing Comprehensive ICT testing plan, covering key areas like penetration, DR, failover etc.	Vulnerability Management Remediation plans for vulnerabilities identified during testing exercises	Data Integrity Outcomes of data reconciliation checks after ICT incidents to evidence data integrity
IT Business Continuity Management 	DORA mandates detailed "ICT business continuity policies" in contrast to BaFin's traditional "business continuity plans" Wider range of scenarios expected under DORA testing requirements Establishing a crisis management function is additionally mandated under DORA	Policy Framework Comprehensive ICT BCM policy covering incident responses, containment, and recovery	Scenario Testing Testing plans which evidence a wide range of scenarios, such as insider threat, outages etc.	Crisis Management Operating model of a crisis management function, with a clearly defined mandate

2. The outputs identified cover key desired capabilities in the BaFin guidance and is not an exhaustive list of all DORA requirements.

Overview of Guidance Notes on Implementation (2/2)

Theme	BaFin Identified Areas of Regulatory Divergence	Key Outputs Expected from In-Scope Firms [3]		
ICT Project Management and Application Development	DORA's ICT project methodology simplifies equivalent BaFin requirements by focussing on impact to critical functions	Project Methodology Documented ICT project management methodology, with focus on critical function impact	ICT Systems Policy Policy framework on ICT system acquisition, development, and maintenance	Source Code Oversight Source code handling policy, including a testing plan prior to use
	DORA's technical standards go into greater detail than BaFin on ICT system acquisition, development, and maintenance			
	Handling of source code from application development is notably more stringent under DORA			
ICT Third-Party Risk Management	Embedding DORA's concept of ICT third-party risk management over traditional outsourcing risk is a key supervisory objective	ICT Third-Party Risk Policy Policy framework to harmonise with ICT third-party risk scope of DORA	Contracts and Due Diligence ICT contracts and vendor due diligence harmonised with DORA's scope	Exit Plans Non-disruptive exit plans for critical service contracts based on severe but plausible scenarios
	DORA goes beyond BaFin on ICT contract minimum requirements and vendor due diligence standards			
	Requirements and goals for exit planning increases significantly with DORA			
Operational Information Security Requirements	Network security and vulnerability handling requirements enhanced under DORA, particularly when linked to critical functions	Network Security Enhanced network security policy for ICT systems supporting critical functions	Encryption Testing Outcomes of network security tests to evidence strength of data encryption	Vulnerability Management Vulnerability management plans with logs to evidence resolution
	Data encryption rules stringer under DORA			
Identity and Access Management Changes	DORA's technical standards stipulate concrete identify management rules and introduces the "need-to-use" principle for access control	Identity Management Firm-wide policy with a clearly mapped identity and account lifecycle	Access Control Access control policy to cover the "need-to-use" principle and ensuring functional separation	Recertifications Calendar of access recertification for critical functions to reflect DORA's six month refresh cycle
	Access control architecture gains greater scrutiny under DORA			

3. The outputs identified cover key desired capabilities in the BaFin guidance and is not an exhaustive list of all DORA requirements.

Contact Us

Marty Clark

m.clark@reply.com

Frederic Gielen

f.gielen@reply.com

Vishwas Khanna

vi.khanna@reply.com