Documentation requirements for financial entities according to DORA

Bundesanstalt für Finanzdienstleistungsaufsicht

Chapter II ICT risk management, section II DORA

Strategies

Article 6 DORA – ICT risk management framework

- **DOR strategy** (Article 6(8) in conjunction with Article 5 (2)(d) DORA)
- **Business strategy** (Article 6(8)(a) DORA)

Article 14 DORA – Communication

- **Communication strategy for ICT-related incidents** (Article 14(3) DORA in conjunction with Article 6(8)(h) DORA)

Chapter IV DORA – Digital operational resilience testing

Article 28-30 DORA

- **Strategy on ICT third-party risk** (Article 28(2) DORA)
- **(optional) ICT multi-vendor strategy** (Article 28(2) in conjunction with Article 6(9) DORA)

Policies

Article 9 DORA – Protection and prevention

- **Information security policy** (Article 9(4)(a) DORA)

Title II - Chapter I RTS RMF - ICT Security policies, procedures, protocols and tools

Section 2	Section 3	Section 4	Section 5	Section 6	Section 7	Section 8
ICT risk management policies (Article 3 RTS RMF)	**ICT asset management policy** (Article 4 RTS RMF in conjunction with Article 9(2) and (4)(c) DORA)	**Policy on encryption and cryptographic controls** (Article 6 and 7 RTS RMF in conjunction with Article 9(2) DORA)	**Policies for ICT operations** (Article 8 RTS RMF in conjunction with Article 9(2) DORA)	**Policies on network security management** (Article 13 RTS RMF)	**ICT project management policy (incl. ICT project risk assessment)** (Article 15 RTS RMF)	**Physical and environmental security policy** (Article 18 RTS RMF)
			Policies for patches and updates (Article 9(4)(f) DORA)	**Policies to protect information in transit** (Article 14 RTS RMF)	**Policy governing the acquisition, development and maintenance of ICT systems** (Article 16(1) RTS RMF)	
					Policies for ICT change management (Article 9(4)(e) DORA)	

Title II - Chapter II RTS RMF - Human resources policy and access control

- **Human resources policy** (Article 19 RTS RMF)
- **Identity management policies** (Article 20 RTS RMF)
- **Policy as part of control of access management rights** (Article 21 RTS RMF in conjunction with Article 9(4)(c) DORA)

Article 11 DORA – Response and recovery

- **ICT business continuity policy** (Article 11 DORA in conjunction with Article 5(2)(e) and Article 8 DORA; Article 24 RTS RMF)
- **(Overall) business continuity policy (incl. BIA)** (Article 11(1) and (5) in conjunction with Article 5(2)(e) DORA)

Article 12 DORA – Backup policies and procedures

- **Backup policies** (Article 12(1)(a) and (2) DORA)

Article 14 DORA – Communication

- **Communication policies for staff (in relation to the ICT risk management framework)** (Article 14(2) DORA)

Article 17-23 DORA

- **ICT-related incident management policy** (Article 22 and 23 RTS RMF)

Chapter IV DORA – Digital operational resilience testing

- **Policies to prioritise, classify and remedy all issues revealed throughout the performance of the tests** (Article 24(5) DORA)
- **Digital operational resilience testing programme** (Article 25(1) DORA in conjunction with Article 24(2) DORA)

Article 28-30 DORA

- **Policy on the use of ICT services supporting critical or important functions** (Article 28(2) and (10) DORA; Article 1 to 11 RTS TPPol)
- **Policy regarding the use of ICT services** (article 5(2)(h) DORA)

Further documentation requirements

Article 6 DORA – ICT risk management framework

- **Report on the ICT risk management framework review** (Article 6(5) DORA in conjunction with Article 27 RTS RMF)
- **(ICT) audit plan incl. follow-up process of critical audit findings** (Article 6(6) to (7) in conjunction with Article 5(2)(f) DORA)

Article 8 DORA – Identification

- **Inventory of all ICT supported business functions, roles and responsibilities** (Article 8(1) and (6) DORA)
- **Inventory of all (critical) information assets and ICT assets** (Article 8(1), (4) and (6) DORA)
- **Inventory of all processes that are dependent on ICT third-party service providers** (Article 8(5) to (6) DORA)

Article 9 DORA – Protection and prevention

- **ICT risk management procedures** (Article 3 RTS RMF)
- **ICT asset management procedure** (Article 5 RTS RMF)
- **Protection measures of cryptographic keys** (Article 9(4)(d) DORA)
- **Register for all certificates and certificate-storing devices for at least ICT assets supporting critical or important functions** (Article 7(4) RTS RMF)
- **Procedures for ICT operations** (Article 8 RTS RMF in conjunction with Article 9(2) DORA)
- **Capacity and performance management procedures** (Article 9 RTS RMF in conjunction with Article 9(2) DORA)
- **Vulnerability management procedures** (Article 10(1) to (2) RTS RMF in conjunction with Article 9(2) DORA)
- **Patch management procedures** (Article 10(3) to (4) RTS RMF in conjunction with Article 9(2) DORA)
- **Data and system security procedure** (Article 11 RTS RMF in conjunction with Article 9(2) DORA)
- **Logging procedures, protocols and tools** (Article 12 RTS RMF)
- **Procedures, protocols and tools on network security management** (Article 13 RTS RMF)
- **Procedures, protocols and tools to protect information in transit** (Article 14 RTS RMF)
- **ICT systems' acquisition, development and maintenance procedure** (Article 16(2) RTS RMF)
- **Procedures and controls for ICT change management** (Article 9(4)(e) DORA; Article 17 RTS RMF)
- **Identity management procedures** (Article 20(1) RTS RMF)
- **Procedures that address access rights** (Article 9(4)(c) DORA)

Article 10 DORA – Detection

- **Mechanisms to promptly detect anomalous activities** (Article 10 DORA in conjunction with Article 23 RTS RMF)

Article 11 DORA – Response and recovery

- **ICT business continuity plans (ICT BCP)** (Article 11(6)(a) DORA; Article 24 and 25 RTS RMF)
- **Documentation of testing of the ICT BCPs** (Article 25(5) RTS RMF)
- **ICT response and recovery plans** (Article 11(3) DORA in conjunction with Article 5(2)(e) DORA; Article 24 and 26 RTS RMF)
- **Records of activities before and during disruption events when their ICT BCPs and ICT response and recovery plans are activated** (Article 11(8) DORA)

Article 12 DORA – Backup policies and procedures

- **Backup procedures** (Article 12(1)(a) and (2) DORA)
- **Restoration and recovery procedures and methods** (Article 12(1)(b) and (2) DORA in conjunction with Article 11(2)(c) DORA)

Article 13 DORA – Learning and evolving

- **ICT security awareness programmes** (Article 13(6) DORA in conjunction with Article 5(2)(g) DORA)
- **Digital operational resilience training** (Article 13(6) DORA in conjunction with Article 5(2)(g) DORA)

Article 14 DORA – Communication

- **Crisis communication plans** (Article 14(1) DORA in conjunction with Article 11(2)(e), (6)(b) and (7) DORA; Article 24 RTS RMF)

Chapter III DORA – ICT-related incident management, classification and reporting

Article 17-23 DORA

- **ICT-related incident management process** (Article 17 DORA in conjunction with RTS CCI; Article 23 RTS RMF)
- **Records of all ICT-related incidents and significant cyber threats** (Article 17(2) DORA in conjunction with RTS CTIR and ITS TIR)

Chapter IV DORA – Digital operational resilience testing

- **Procedures to prioritise, classify and remedy all issues revealed throughout the performance of the tests** (Article 24(5) DORA)
- **Validation methodologies** (Article 24(5) DORA)

Article 28-30 DORA

- **Register of information** (Article 28(3) DORA in conjunction with ITS RoI)
- **Exit plans** (Article 28(8) DORA; Article 10 RTS TPPol)

Colour legend

Strategy | Policy* | Policy* | Further document | Overall document

Abbreviation of relevant legal texts:

DORA = **D**igital **O**perational **R**esilience **A**ct
RTS = **R**egulatory **T**echnical **S**tandard
ITS = **I**mplementing **T**echnical **S**tandard

RTS RMF = RTS ICT **R**isk **M**anagement **F**ramework
RTS CCI = RTS **C**lassification **C**riteria **I**ncidents
RTS CTIR = RTS **C**ontent and **T**ime limits **I**ncident **R**eporting
ITS TIR = ITS **T**emplates **I**ncident **R**eporting
RTS TPPol = RTS ICT **T**hird-**P**arty **Pol**icy
ITS RoI = ITS **R**egister **o**f **I**nformation

***Remark**: The overview contains the titles from the original English text.
In the English version, there are no formal distinctions between different policy terms compared to the German version, which is why these are not further differentiated linguistically here.
In addition, certain requirements of DORA, that are only applicable to few financial entities, are not subject of this overview.
Further information is included in the accompanying notes.