

DORA Documentation Requirements Checklist

Document	Legal/ Regulatory Requirements	Created?	Up to Date?	Implemented?
Strategy	Legal/ Regulatory Requirements	Created?	Up to Date?	Implemented?
DOR-Strategy	Article 6 (8) i.c.w. Article 5 (2)(d) DORA			
Communication strategy for ICT-related incidents	Article 14 (3) i.c.w. Article 6 (8)(h) DORA			
Strategy on ICT third-party risk	Article 28 (2) DORA			
(optional) ICT multi-vendor strategy	Article 28 (2) i.c.w. Article 6 (9) DORA			
Policy	Legal/ Regulatory Requirements	Created?	Up to Date?	Implemented?
Information security policy	Article 9 (4)(a) DORA			
ICT risk management policies	Article 3 RTS RMF			
ICT asset management policy	Article 4 RTS RMF i.c.w. Article 9 (2) and 4(c) DORA			
Policy on encryption and cryptographic controls	Article 6 and 7 RTS RMF i.c.w. Article 9 (2) DORA			
Policies for ICT operations	Article 8 RTS RMF i.c.w. Article 9 (2) DORA			
Policies for patches and updates	Article 9 (4)(f) DORA			
Policies on network security management	Article 13 RTS RMF			
Policies to protect information in transit	Article 14 RTS RMF			
ICT project management policy (incl. ICT project risk assessment)	Article 15 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			
Physical and environmental security policy	Article 18 RTS RMF			
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 i.c.w. Article 9 (4)(c) DORA			
ICT business continuity policy	Article 11 DORA i.c.w. Article 5 (2)(e) and Article 8 DORA; Article 24 RTS RMF			
Backup policies	Article 12 (1)(a) and (2) DORA			
Communication policies for staff (in relation to the ICT risk management framework)	Article 14 (2) DORA			
ICT-related incident management policy	Article 22 and 23 RTS RMF			
Policies to prioritise, classify and remedy all issues revealed throughout the performance of the tests	Article 24 (5) DORA			

DORA Documentation Requirements Checklist

Document	Legal/ Regulatory Requirements	Created?	Up to Date?	Implemented?
Policy on the use of ICT services supporting critical or important functions	Article 28 (2) and 10 DORA; Article 1-11 RTS TPPol			
Further document	Legal/ Regulatory Requirements	Created?	Up to Date?	Implemented?
Report on the ICT risk management framework review	Article 6 (5) DORA i.c.w. Article 27 RTS RMF			
(ICT) audit plan incl. follow-up process of critical audit findings	Article 6 (6) and 7 i.c.w. Article 5 (2)(f) DORA			
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) and 6 DORA			
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 i.c.w. Article 9 (2) DORA			
Capacity and performance management procedures	Article 9 RTS RMF i.c.w. Article 9 (2) DORA			
Vulnerability management procedures	Article 10 (1) and 2 RTS RMF i.c.w. Article 9 (2) DORA			
Patch management procedures	Article 10 (3) and 4 RTS RMF i.c.w. Article 9 (2) DORA			
Data and system security procedure	Article 11 RTS RMF i.c.w. 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			

DORA Documentation Requirements Checklist

Document	Legal/ Regulatory Requirements	Created?	Up to Date?	Implemented?
Identity management procedures	Article 20 (1) RTS RMF			
Procedures that address access rights	Article 9 (4)(c) DORA			
Mechanisms to promptly detect anomalous activities	Article 10 DORA i.c.w. Article 23 RTS RMF			
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 i.c.w. Article 5 (2)(e) DORA; Article 24 u. 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			
Backup procedures	Article 12 (1)(a) and (2) DORA			
Restoration and recovery procedures and methods	Article 12 (1)(b) and (2) DORA i.c.w. Article 11 (2)(c) DORA			
ICT security awareness programmes	Article 13 (6) DORA i.c.w. Article 5 (2)(g) DORA			
Digital operational resilience training	Article 13 (6) DORA i.c.w. Article 5 (2)(g) DORA			
Crisis communication plans	Article 14 (1) DORA i.c.w. Article 11 (2)(e), (6)(b) and 7 DORA; Article 24 RTS RMF			
ICT-related incident management process	Article 17 DORA; Article 23 RTS RMF			
Records of all ICT-related incidents and significant cyber threats	Article 17 (2) DORA			
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			
Register of information	Article 28 (3) DORA i.c.w. ITS RoI			
Exit plans	Article 28 (8) DORA; Article 10 RTS TPPol			
Overall document	Legal/ Regulatory Requirements	Created?	Up to Date?	Implemented?
Business Strategy	Article 6 (8)(a) DORA			
(Overall) business continuity policy (incl. BIA)	Article 11 (1) and 5 i.c.w. Article 5 (2)(e) DORA			
Digital operational resilience testing programme	Article 25 (1) DORA i.c.w. Article 24 (2) DORA			
Policy regarding the use of ICT services	Article 5 (2)(h) DORA			