DORA Temple 2.0

- Overview of strategies, policies, ICT security policies and procedures -

Strategy
ICT security policy
Procedure/ Process

Business strategy *Art. 6(8)(a) DORA*

Digital operational resilience strategy *Art. 6(8) DORA*

Strategy on ICT third-party risk *Art. 28(2) DORA*

Multi-vendor strategy optional, *Art. 6(9) DORA*

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

Exit strategy for ICT services supporting critical or important functions *Art. 28(8) DORA in conjunction with Art. 10 RTS TPRM*

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16*	17	18	19	20	21	22	23	24	25	26
Information security policy	ICT risk management	ICT asset management	Human resources policy	Identity management	Access control	Physical and environmental security	Encryption and cryptography	ICT operations security	Network security	Securing information in transit	Patches and updates	ICT change management	ICT project management	ICT systems acquisition, development, and maintenance	End-user computing (EUC)†	ICT-related incident management	Internal and external communication policy†	Overall business continuity policy	ICT business continuity policy	Backup policy	Digital operational resilience testing programme	Test findings remediation policy†	TLPT policy	ICT third-party services policy†	ICT third-party policy for critical or important functions†
Art. 9(4)(a) DORA	Art. 3 RTS RMF	Art. 4 RTS RMF	Art. 19 RTS RMF	Art. 20 RTS RMF	Art. 21 RTS RMF	Art. 18 RTS RMF	Art. 6 and 7 RTS RMF	Art. 8 RTS RMF	Art. 13 RTS RMF	Art. 14 RTS RMF	Art. 9(4)(f) DORA	Art. 9(4)(e) DORA	Art. 15 RTS RMF	Art. 16(1) RTS RMF	Art. 16(9) RTS RMF	Art. 22 and 23 RTS RMF	Art. 14(2) DORA	Art. 11(1) and (5) DORA	Art. 11 DORA, Art. 24 RTS RMF	Art. 12(1)(a) DORA	Art. 24(1) DORA	Art. 24(5) DORA	Art. 26 DORA	Art. 5(2)(h) DORA	Art. 28(2) DORA, RTS TPRM
P1 P2 P3	P4		P5	P6		P7 P8 P9 P10	P11	P12	P13 P14	P15	P16	P17 P18		P19 P20	P21 P22	P23									

*practical interpretation of pillar 15 †practical name, legal wording see article

Procedure documents for the pillars

P1 ICT risk assessment (Art. 3(b) RTS RMF)
P2 ICT risk treatment (Art. 3(c) RTS RMF)
P3 Follow-up process (Art. 6(7) DORA)
P4 ICT asset management (Art. 5 RTS RMF)
P5 Identity management (Art. 20(1) RTS RMF)
P6 Access rights (Art. 9(4)(c) DORA)
P7 ICT operations management (Art. 8 RTS RMF)
P8 Capacity and performance mgmt. (Art. 9 RTS RMF)
P9 Logging (Art. 12 RTS RMF)
P10 Data/system security (Art. 11 RTS RMF)
P11 Network security mgmt. (Art. 13 RTS RMF)
P12 Protection in transit (Art. 14 RTS RMF)
P13 Vulnerability management (Art. 10(1) and (2) RTS RMF)
P14 Patch management (Art. 10(3) and (4) RTS RMF)
P15 ICT change management (Art. 9(4)(e) DORA)
P16 Acquisition/dev./maintenance (Art. 16(2) RTS RMF)
P17 ICT-related incident mgmt. process (Art. 17 DORA)
P18 Incident classification (Art. 17(3)(b) DORA)
P19 ICT business continuity management (Art. 11(2) DORA)
P20 Crisis communication/ crisis management (Art. 11(7) DORA)
P21 Backup procedures (Art. 12(1)(a) DORA)
P22 Restoration and recovery procedures (Art. 12(1)(b) DORA)
P23 Test findings remediation† (Art. 24(5) DORA)

Own illustration, partly created with the help of AI