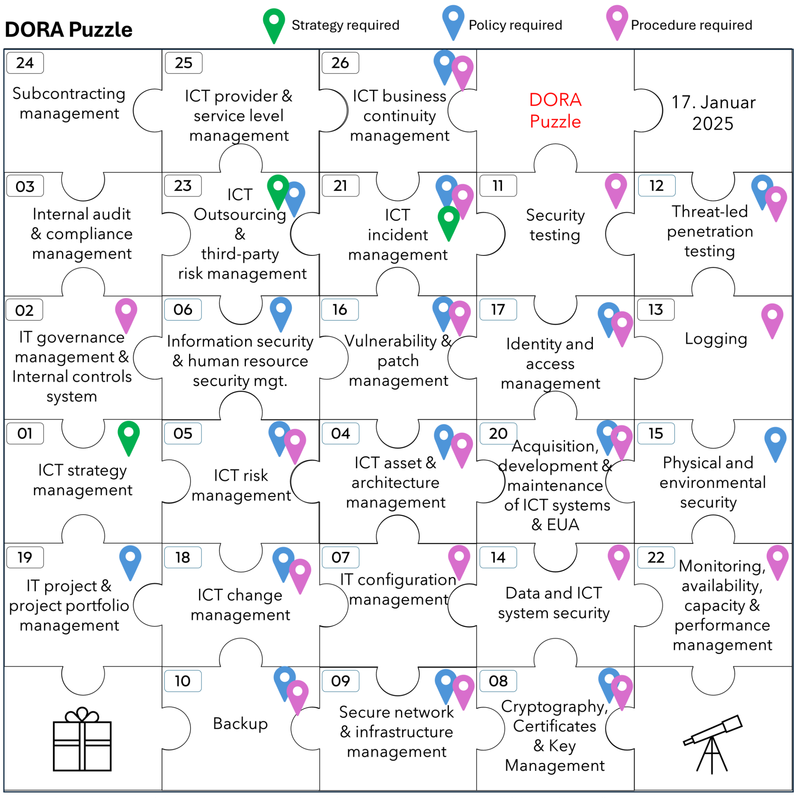
DORA strategies, policies & procedures



	Domain	Strategys, policies & procedures	DORA reference
1	ICT strategy management	- Business strategy with defined business objectives - DOR strategy including defined ICT objectives	(Art. 6 Abs. 8 (a) DORA) (Art. 6 Abs. 8 DORA)
2	IT governance management & Internal controls system	- Procedures to exchange cyber threat information and intelligence	(Art. 45 Abs. 1 DORA)
3	Internal audit & compliance management	- n/a	n/a
4	ICT asset & architecture management	- Policy on management of ICT assets - ICT asset management procedure including the criteria to perform the criticality assessment	(Art. 4 Abs. 1 RTS risk mgt.) (Art. 5 Abs. 1 RTS risk mgt.)
5	ICT risk management	- Policies and procedures concerning ICT risk management - Procedure and the methodology to conduct the ICT risk assessments - ICT risk treatment procedure	(Art. 3 Abs. 1 RTS risk mgt.) (Art. 3 Abs. 1 (b) RTS risk mgt.) (Art. 3 Abs. 1 (c) RTS risk mgt.)
6	Information security & human resource security management	- Human resource (security) policy - Information security policy - Clear desk policy and clear screen policy	(Art. 19 Abs. 1 RTS risk mgt.) (Art. 9 Abs. 4 (a) DORA) (Art. 18 Abs. 2 (e) RTS risk mgt.)
7	IT configuration management	- Policies and procedures to manage the ICT operations of ICT assets	(Art. 8 Abs. 2 RTS risk mgt.)
8	Cryptography, Certificates & Key Management	- Policy on encryption and cryptographic controls	(Art. 6 Abs. 3 RTS risk mgt.)
9	Secure network & infrastructure management	- Policies and procedures on network security management - Policies & procedures to protect information in transit - Procedures to assess compliance with requirements to protect information in transit	(Art. 13 Abs. 1 RTS risk mgt.) (Art. 14 Abs. 1 RTS risk mgt.) (Art. 14 Abs. 1 (a) RTS risk mgt.)
10	Backup	- Backup policies and procedures - Procedures for ICT system restart, rollback and recovery - Restoration and recovery procedures	(Art. 12 Abs. 1 (a) DORA) (Art. 8 Abs. 2 (c) RTS risk mgt.) (Art. 11 Abs, 2 (c) DORA)
11	Security testing	- Procedures and policies to prioritize, classify and remedy all issues revealed throughout the performance of security tests	(Art. 24 Abs. 5 DORA)
12	Threat-led penetration testing (TLPT)	- TLPT procedures for future back-up restauration - Policy for the management of internal testers in a TLPT	(Art. 5 Abs. 2 (v) RTS TLPT) (Art. 11 Abs. 1 (a) RTS TLPT)
13	Logging	- Logging procedures	(Art. 12 Abs. 1RTS risk mgt.)
14	Data and ICT system security	- Data and ICT system security procedure	(Art. 11 Abs. 1 RTS risk mgt.)
15	Physical and environmental security	- Physical and environmental security policy - Policies that limit the physical or logical access	(Art. 18 Abs. 1 RTS risk mgt.) (Art. 9 Abs. 4 (c) DORA)
16	Vulnerability & patch management	- Policies for patches and updates - Vulnerability management procedures - Procedures for disclosure of vulnerabilities - Patch management procedures - Emergency procedures for the patching and updating of ICT assets - Escalation procedures in case the deadline for installation of patches and updates cannot be met	(Art. 9 Abs. 4 (f) DORA) (Art. 10 Abs. 1 RTS risk mgt.) (Art. 10 Abs. 2 (e) RTS risk mgt.) (Art. 10 Abs. 4 RTS risk mgt.) (Art. 10 Abs. 4 (b) RTS risk mgt.) (Art. 10 Abs. 4 (d) RTS risk mgt.)
17	Identity and access management	- Policies and procedures that address access rights - Identity management policies and procedures - Account management procedures - Policy on control of access management rights - Policies for strong authentication mechanisms	(Art. 9 Abs. 4 (c) DORA) (Art. 20 Abs. 1 RTS risk mgt.) (Art. 21 Abs. 1 (e) RTS risk mgt.) (Art. 21 Abs. 1 RTS risk mgt.) (Art. 9 Abs. 4 (d) DORA)
18	ICT change management	- Policies and procedures for ICT change management - ICT change management procedures - Fall-back procedures, procedures for aborting changes and procedures for recovering from changes - Procedures to manage emergency changes - Procedures to document, re-evaluate, assess and approve emergency changes	(Art. 9 Abs. 4 (e) DORA) (Art. 17 Abs. 1 RTS risk mgt.) (Art. 17 Abs. 2 (e) RTS risk mgt.) (Art. 17 Abs. 2 (f) RTS risk mgt.) (rt. 17 Abs. 2 (g) RTS risk mgt.)
19	IT project & project portfolio management	- ICT project management policy	(Art. 15 Abs. 1 RTS risk mgt.)
20	Acquisition, development and maintenance of ICT systems and EUA	- Policy governing the acquisition, development and maintenance of ICT systems - ICT systems' acquisition, development and maintenance procedure	(Art. 16 Abs. 1 RTS risk mgt.) (Art. 16 Abs. 2 RTS risk mgt.)
21	ICT incident management	- Communication strategy for ICT-related incidents - ICT-related incident management policy - Procedures to ensure a consistent and integrated monitoring, handling and follow-up of ICT- related incidents - Procedures to identify, track, log, categorise and classify ICT-related incidents - Escalation procedures for ICT-related incidents - ICT-related incident response procedures - Procedures for handling errors	(Art. 14 Abs. 3 DORA) (Art. 22 Abs. 1 RTS risk mgt.) (Art. 17 Abs. 2 DORA) (Art. 17 Abs. 3 (b) DORA) (Art. 17 Abs. 3 (d) DORA) (Art. 17 Abs. 3 (f) DORA) (Art. 8 Abs. 2 (c) (i) RTS risk mgt.)
22	Monitoring, availability, capacity & performance management	- Policies and procedures to manage the ICT operations of ICT assets - Capacity and performance management procedures - Procedures to limit, lock and terminate system and remote sessions - Resource optimisation and monitoring procedures	(Art. 8 Abs. 2 RTS risk mgt.) (Art. 9 Abs. 1 RTS risk mgt.) (Art. 13 Abs. 1 RTS risk mgt.) (Art. 9 Abs. 1 RTS risk mgt.)
23 24 25	ICT outsourcing & third-party risk management Subcontracting management ICT provider & service level management	- Strategy on ICT third-party risk and multi-vendor strategy - Exit strategies - Policy on the use of ICT services supporting critical or important functions provided by ICT third-party service providers	(Art. 28 Abs. 2 DORA) (Art. 28 Abs. 8 DORA) (Art. 28 Abs. 2 DORA) (Art. 1 RTS Policy on use of ICT services)
26	ICT business continuity management	- Overall business continuity policy - ICT business continuity policy - Communication policies for staff - Procedures for ICT business continuity management - Procedures to manage internal and external crisis communications - Procedures to verify the to respond adequately to BCM scenarios - Escalation procedures for the implementation of the ICT business continuity policy	(Art. 11 Abs. 5 DORA) (Art. 11 Abs. 1 DORA) (Art. 14 Abs. 2 DORA) (Art. 11 Abs, 2 DORA) (Art. 11 Abs. 7 DORA) (Art. 25 Abs. 2 (e) RTS risk mgt.) (Art. 24 Abs. 1 (e) RTS risk mgt.)