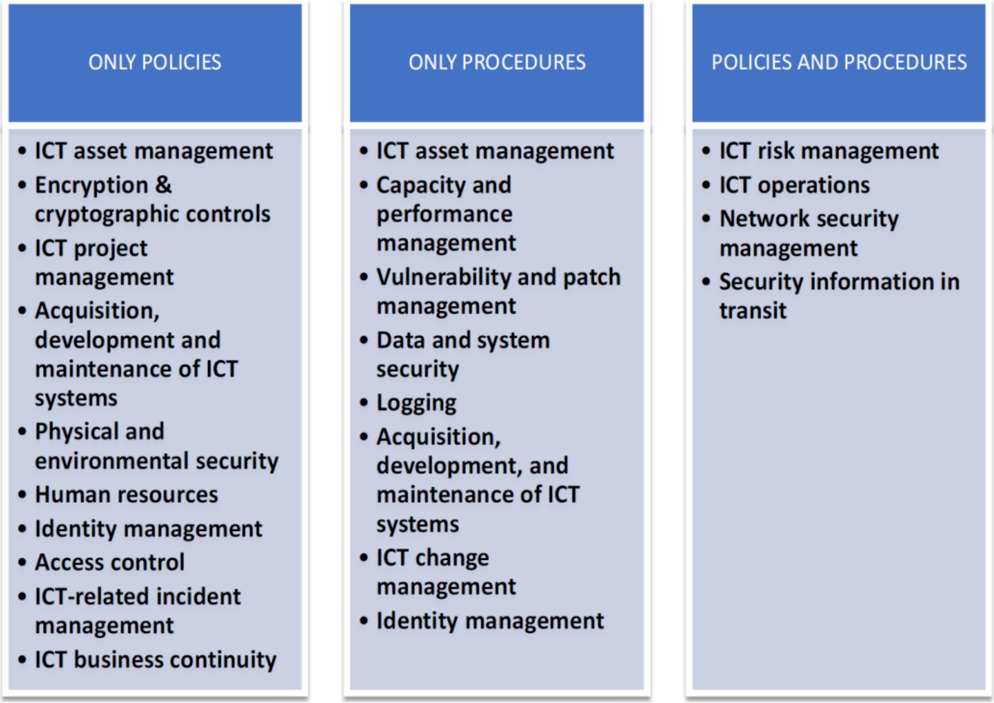
Original figure of DORA policies & procedures in RTS risk management …



ONLY POLICIES

- ICT asset management
- Encryption & cryptographic controls
- ICT project management
- Acquisition, development and maintenance of ICT systems
- Physical and environmental security
- Human resources
- Identity management
- Access control
- ICT-related incident management
- ICT business continuity

ONLY PROCEDURES

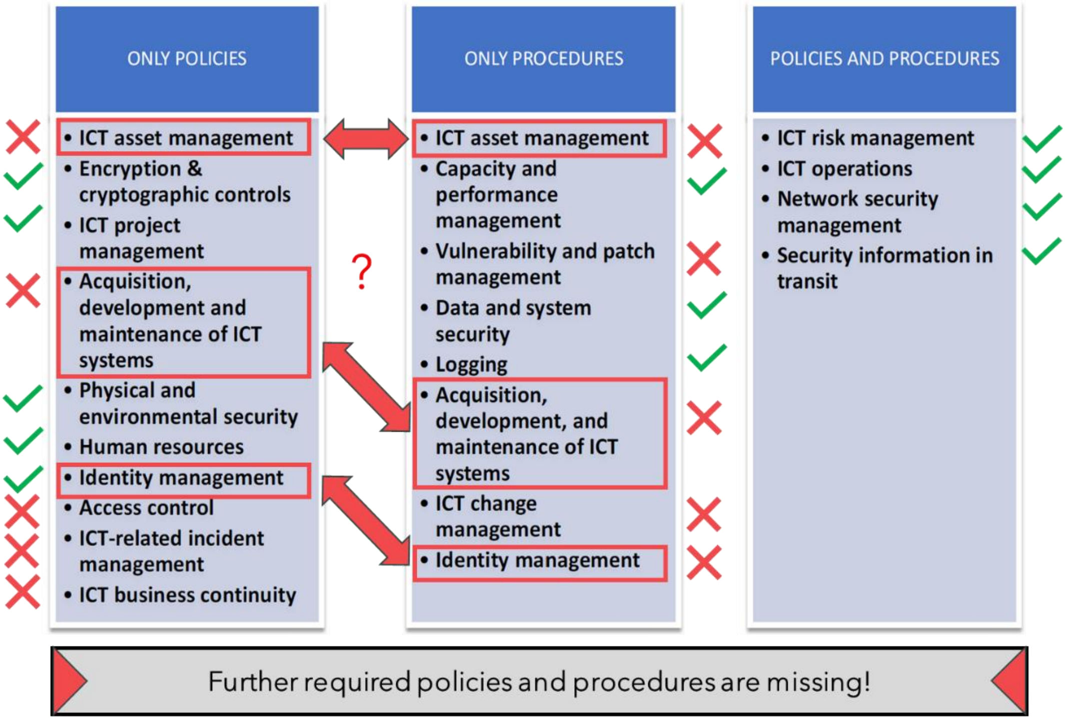
- ICT asset management
- Capacity and performance management
- Vulnerability and patch management
- Data and system security
- Logging
- Acquisition, development, and maintenance of ICT systems
- ICT change management
- Identity management

POLICIES AND PROCEDURES

- ICT risk management
- ICT operations
- Network security management
- Security information in transit

Quelle: JC 2023 86, Final report, Draft Regulatory Technical Standards to further harmonise ICT risk management tools, methods, processes and policies as mandated under Articles 15 and 16(3) of Regulation (EU) 2022/2554, Seite 14, 2024

… is unfortunately misleading and incomplete.



ONLY POLICIES

- ✗ ICT asset management
- ✓ Encryption & cryptographic controls
- ✓ ICT project management
- ✗ Acquisition, development and maintenance of ICT systems
- ✓ Physical and environmental security
- ✓ Human resources
- ✓ Identity management
- ✗ Access control
- ✗ ICT-related incident management
- ✗ ICT business continuity

?

ONLY PROCEDURES

- ICT asset management ✗
- Capacity and performance management ✓
- Vulnerability and patch management ✗
- Data and system security ✓
- Logging ✓
- Acquisition, development, and maintenance of ICT systems ✗
- ICT change management ✗
- Identity management ✗

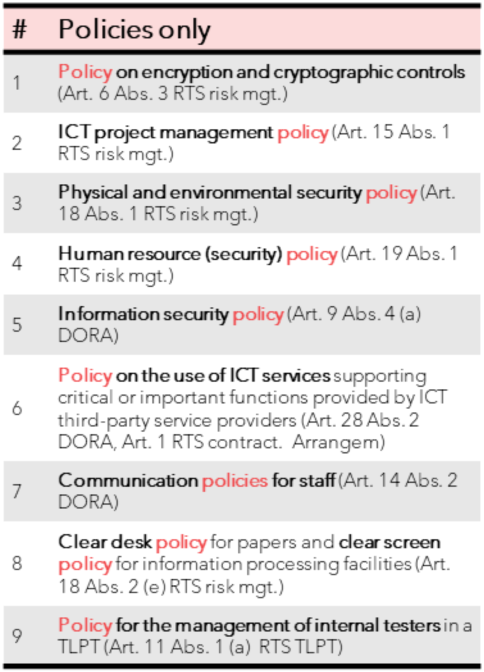
POLICIES AND PROCEDURES

- ICT risk management ✓
- ICT operations ✓
- Network security management ✓
- Security information in transit ✓

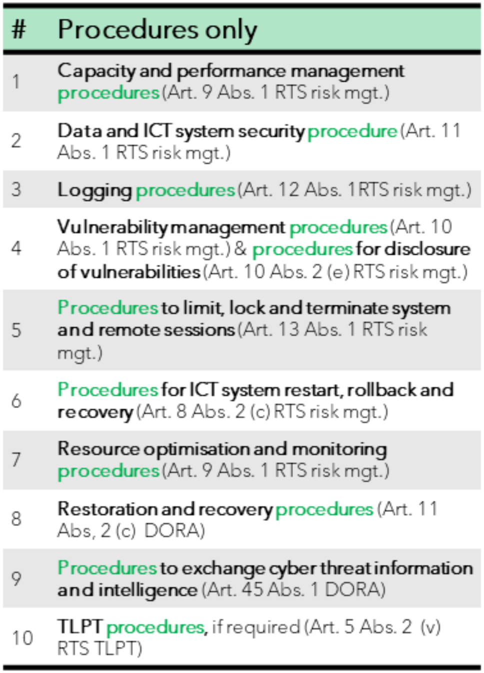
Further required policies and procedures are missing!

Eigene Darstellung in Anlehnung an Final report, Draft Regulatory Technical Standards to further harmonise ICT risk management tools, methods, processes and policies as mandated under Articles 15 and 16(3) of Regulation (EU) 2022/2554, Seite 14, 2024

You should better refer to my overview on “policies and procedures only”…



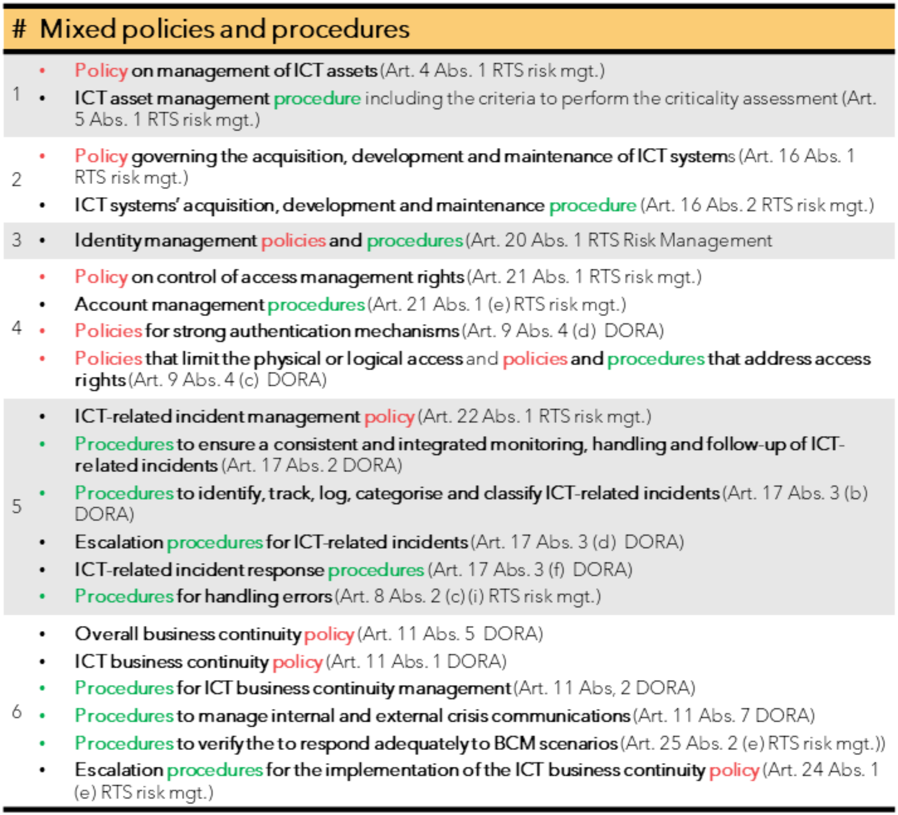
#	Policies only
1	Policy on encryption and cryptographic controls (Art. 6 Abs. 3 RTS risk mgt.)
2	ICT project management policy (Art. 15 Abs. 1 RTS risk mgt.)
3	Physical and environmental security policy (Art. 18 Abs. 1 RTS risk mgt.)
4	Human resource (security) policy (Art. 19 Abs. 1 RTS risk mgt.)
5	Information security policy (Art. 9 Abs. 4 (a) DORA)
6	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. 1 RTS contract. Arrangem)
7	Communication policies for staff (Art. 14 Abs. 2 DORA)
8	Clear desk policy for papers and clear screen policy for information processing facilities (Art. 18 Abs. 2 (e) RTS risk mgt.)
9	Policy for the management of internal testers in a TLPT (Art. 11 Abs. 1 (a) RTS TLPT)



#	Procedures only
1	Capacity and performance management procedures (Art. 9 Abs. 1 RTS risk mgt.)
2	Data and ICT system security procedure (Art. 11 Abs. 1 RTS risk mgt.)
3	Logging procedures (Art. 12 Abs. 1RTS risk mgt.)
4	Vulnerability management procedures (Art. 10 Abs. 1 RTS risk mgt.) & procedures for disclosure of vulnerabilities (Art. 10 Abs. 2 (e) RTS risk mgt.)
5	Procedures to limit, lock and terminate system and remote sessions (Art. 13 Abs. 1 RTS risk mgt.)
6	Procedures for ICT system restart, rollback and recovery (Art. 8 Abs. 2 (c) RTS risk mgt.)
7	Resource optimisation and monitoring procedures (Art. 9 Abs. 1 RTS risk mgt.)
8	Restoration and recovery procedures (Art. 11 Abs, 2 (c) DORA)
9	Procedures to exchange cyber threat information and intelligence (Art. 45 Abs. 1 DORA)
10	TLPT procedures, if required (Art. 5 Abs. 2 (v) RTS TLPT)

Eigene Darstellung, © Copyright 2024 | Dr. Marlen Hofmann

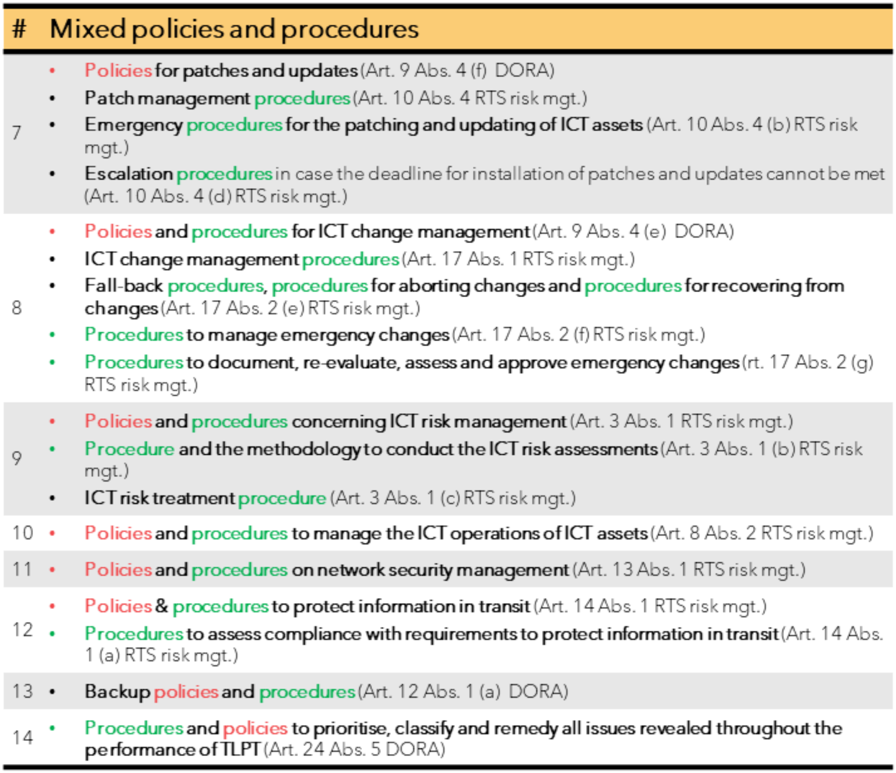
… and “mixed policies and procedures” (1 of 2)



#	Mixed policies and procedures
1	• Policy on management of ICT assets (Art. 4 Abs. 1 RTS risk mgt.) • ICT asset management procedure including the criteria to perform the criticality assessment (Art. 5 Abs. 1 RTS risk mgt.)
2	• Policy governing the acquisition, development and maintenance of ICT systems (Art. 16 Abs. 1 RTS risk mgt.) • ICT systems' acquisition, development and maintenance procedure (Art. 16 Abs. 2 RTS risk mgt.)
3	• Identity management policies and procedures (Art. 20 Abs. 1 RTS Risk Management
4	• Policy on control of access management rights (Art. 21 Abs. 1 RTS risk mgt.) • Account management procedures (Art. 21 Abs. 1 (e) RTS risk mgt.) • Policies for strong authentication mechanisms (Art. 9 Abs. 4 (d) DORA) • Policies that limit the physical or logical access and policies and procedures that address access rights (Art. 9 Abs. 4 (c) DORA)
5	• ICT-related incident management policy (Art. 22 Abs. 1 RTS risk mgt.) • Procedures to ensure a consistent and integrated monitoring, handling and follow-up of ICT-related incidents (Art. 17 Abs. 2 DORA) • Procedures to identify, track, log, categorise and classify ICT-related incidents (Art. 17 Abs. 3 (b) DORA) • Escalation procedures for ICT-related incidents (Art. 17 Abs. 3 (d) DORA) • ICT-related incident response procedures (Art. 17 Abs. 3 (f) DORA) • Procedures for handling errors (Art. 8 Abs. 2 (c) (i) RTS risk mgt.)
6	• Overall business continuity policy (Art. 11 Abs. 5 DORA) • ICT business continuity policy (Art. 11 Abs. 1 DORA) • Procedures for ICT business continuity management (Art. 11 Abs, 2 DORA) • Procedures to manage internal and external crisis communications (Art. 11 Abs. 7 DORA) • Procedures to verify the to respond adequately to BCM scenarios (Art. 25 Abs. 2 (e) RTS risk mgt.)) • Escalation procedures for the implementation of the ICT business continuity policy (Art. 24 Abs. 1 (e) RTS risk mgt.)

Eigene Darstellung, © Copyright 2024 | Dr. Marlen Hofmann

… and “mixed policies and procedures” (2 of 2)



#	Mixed policies and procedures
7	• Policies for patches and updates (Art. 9 Abs. 4 (f) DORA) • Patch management procedures (Art. 10 Abs. 4 RTS risk mgt.) • Emergency procedures for the patching and updating of ICT assets (Art. 10 Abs. 4 (b) RTS risk mgt.) • Escalation procedures in case the deadline for installation of patches and updates cannot be met (Art. 10 Abs. 4 (d) RTS risk mgt.)
8	• Policies and procedures for ICT change management (Art. 9 Abs. 4 (e) DORA) • ICT change management procedures (Art. 17 Abs. 1 RTS risk mgt.) • Fall-back procedures, procedures for aborting changes and procedures for recovering from changes (Art. 17 Abs. 2 (e) RTS risk mgt.) • Procedures to manage emergency changes (Art. 17 Abs. 2 (f) RTS risk mgt.) • Procedures to document, re-evaluate, assess and approve emergency changes (rt. 17 Abs. 2 (g) RTS risk mgt.)
9	• Policies and procedures concerning ICT risk management (Art. 3 Abs. 1 RTS risk mgt.) • Procedure and the methodology to conduct the ICT risk assessments (Art. 3 Abs. 1 (b) RTS risk mgt.) • ICT risk treatment procedure (Art. 3 Abs. 1 (c) RTS risk mgt.)
10	• Policies and procedures to manage the ICT operations of ICT assets (Art. 8 Abs. 2 RTS risk mgt.)
11	• Policies and procedures on network security management (Art. 13 Abs. 1 RTS risk mgt.)
12	• Policies & procedures to protect information in transit (Art. 14 Abs. 1 RTS risk mgt.) • Procedures to assess compliance with requirements to protect information in transit (Art. 14 Abs. 1 (a) RTS risk mgt.)
13	• Backup policies and procedures (Art. 12 Abs. 1 (a) DORA)
14	• Procedures and policies to prioritise, classify and remedy all issues revealed throughout the performance of TLPT (Art. 24 Abs. 5 DORA)

Eigene Darstellung, © Copyright 2024 | Dr. Marlen Hofmann