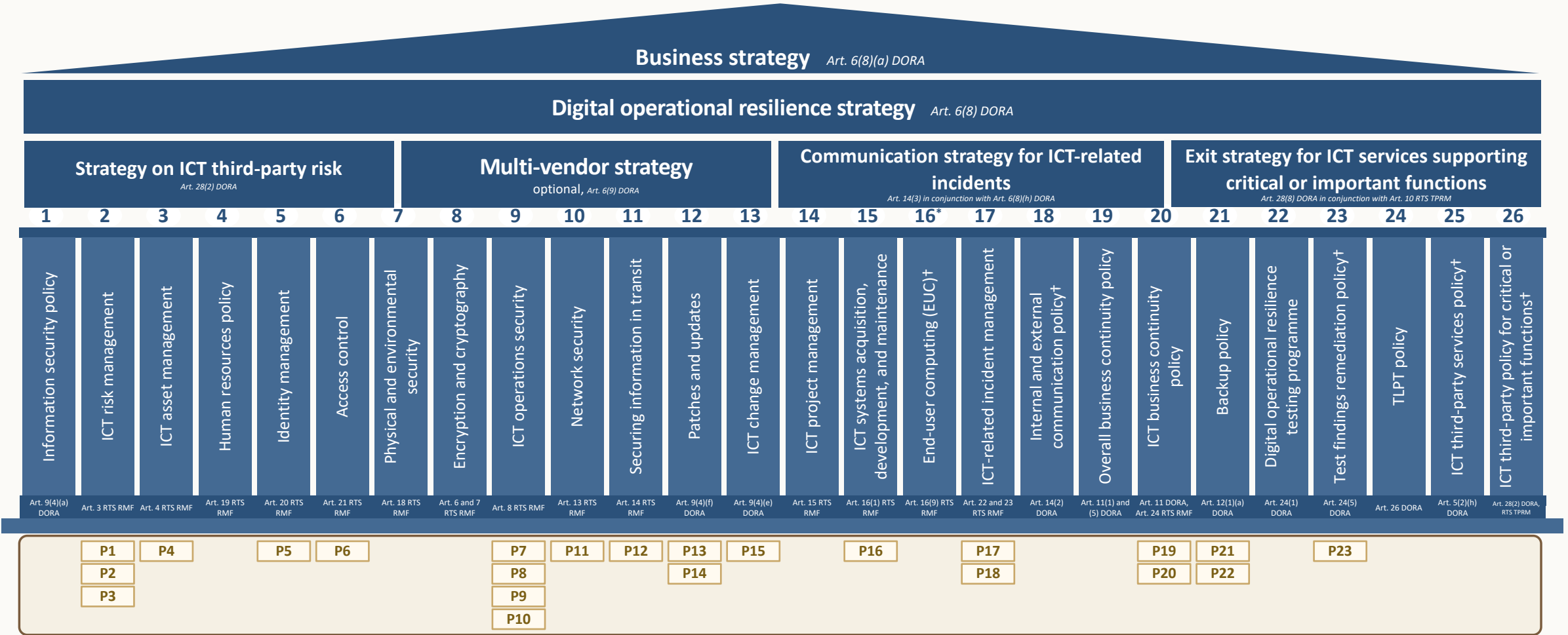


DORA Temple 2.0

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

- Strategy
- ICT security policy
- Procedure/ Process



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)

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