DORA mandatory time specifications and time limits

24 Subcontracting management

25 ICT provider & service level management

26 ICT business continuity management

- test ICT BC plans and ICT response & recovery plans at least yearly
- central securities depositories shall ensure that the recovery time objective for their critical or important functions shall not be longer than two hours.
- trading venues shall ensure that their ICT business continuity arrangements allow trading can be resumed within or close to two hours and that maximum amount of data that may be lost is close to zero.

DORA Puzzle

17. Januar 2025

03 Internal audit & compliance management

23 ICT outsourcing & third-party risk management

- report at least yearly to the competent authorities
- maintain the information in the register of information at least 5 years after the termination of the provision of the ICT services
- review the policy at least once a year,

21 ICT incident management

- Prioritise alerts to allow the detected ICT-related incidents to be managed within the expected resolution time, both during and outside working hours
- The materiality threshold for the duration and service downtime criterion shall be met where
  - duration of the incident is longer than 24 hours; or
  - service downtime is > 2 hours for ICT services that support critical or important functions.
- Recurring incidents shall be considered as one major incident where the incidents have occurred at least twice within 6 months
- Financial entities shall assess the existence of recurring incidents on a monthly basis.
- Initial report shall be submitted as early as possible within 4 hours from the moment of classification of incident as major, but no later than 24 hours from time of
- Intermediate report shall be submitted within 72 hours from classification of incident as major,
- Final report shall be submitted no later than 1 month from the classification as major, unless the incident has not been resolved. In that latter case, the final report shall be submitted the day after the incident has been re-solved permanently.
- Where the deadline falls on a weekend day or a bank holiday, financial entities may submit the intermediate or final reports within one hour following regular starting time of the next working day.
- Where unable to submit the initial notification, intermediate report or final report within the timelines, financial entities shall inform competent authority without undue delay, but no later than 24 hours, and shall explain the reasons for delay

11 Security testing

- Financial entities shall ensure, at least yearly, that appropriate tests are conducted on all ICT systems and applications supporting critical or important functions.

12 Threat-led penetration testing

- submit initiation documents within three months from having received a notification
- specification document shall be submitted to TLPT authority within six months
- duration of the active red team testing phase shall be in any case at least twelve weeks
- testers shall report at least weekly on the progress of TLPT
- Within four weeks from the end of the active red team testing phase, the testers shall submit a red team test report
- Upon receipt of the red team test report, and no later than four weeks after, the blue team shall submit a blue team test report
- Within four weeks from sharing blue team test report, the blue team shall carry out replay of the offensive and defensive actions
- Within 12 weeks from completion of the active red team testing phase, the control team shall submit the test summary report
- Within 16 weeks from the ending of the active red team testing phase, the financial entity shall provide the remediation plans
- require that all members of the test team have been employed for the preceding two years;
- Within 20 working days from information on a future conduct of a TLPT, the TLPT authorities may either express their interest
- the staff of the threat intelligence provider shall be composed of at least a manager with at least five years of experience in threat intelligence, as well as at least one additional member with at least two years of experience in threat intelligence;
- for external testers, the staff of the red team shall be composed of at least a manager, with at least five years of experience in threat intelligence-led red team testing as well as at least two additional testers, each with experience of at least two years;

02 IT governance management & Internal controls system

- Senior ICT staff shall report at least yearly to the management body on the findings referred to in paragraph 3 and put forward recommendations.

06 Information security & human resource security mgt.

16 Vulnerability & patch management

- performance of automated vulnerability scanning and assessments on ICT assets. For the ICT assets supporting critical or important functions it shall be performed at least on a weekly basis;

17 Identity and access management

- update of access rights at least once a year for all ICT systems, and at least every six months for ICT systems supporting critical or important functions;

13 Logging

01 ICT strategy management

05 ICT risk management

- Review risk scenarios at least yearly
- The ICT risk management framework shall be reviewed at least once a year as well as upon the occurrence of major ICT-related incidents
- Ensure assessment of accepted residual ICT risks at least once a year

04 ICT asset & architecture management

- Classify assets at least yearly
- Update inventories periodically and every time any major change occurs

20 Acquisition, development & maintenance of ICT systems & EUA

15 Physical and environmental security

19 IT project & project portfolio management

18 ICT change management

07 IT configuration management

14 Data and ICT system security

- Financial entities shall on a regular basis, and at least yearly, conduct a specific ICT risk assessment on all legacy ICT systems and, in any case before and after connecting technologies, applications or systems

22 Monitoring, availability, capacity & performance ,management

10 Backup

09 Secure network & infrastructure management

- For ICT systems supporting critical or important functions, verify existing firewall rules and connection filters at least every six months
- Ensure the performance of reviews of the network architecture and of the network security design once a year

08 Cryptography, Certificates & Key Management

© Copyright 2024 | Dr. Marlen Hofmann| Alle Inhalte, insbesondere Texte, Fotografien und Grafiken sind urheberrechtlich geschützt. Alle Rechte, einschließlich der Vervielfältigung, Veröffentlichung, Bearbeitung und Übersetzung, bleiben vorbehalten.