Roundtable
Digital Operational Resilience Act (DORA)

[26 oktober 2023]

KENNISGROEP BETALINGSVERKEER

NOREA
DE BEROEPSORGANISATIE VAN IT-AUDITORS

DORA

Introductie

Victoria van der Mark

- Toezichthouder Operational & IT Risk
- Achtergrond in IT-audit (RE), informatiebeveiliging en cyber
- Lid programmateam DORA bij de AFM

Sean Weggelaar

- Toezichthouder Operational & IT Risk
- Achtergrond in financiele sector, project management & IT auditing
- DORA programmamanager bij de AFM

Disclaimer

Informatie die in deze presentatie wordt gedeeld is gebaseerd op de huidige stand van zaken van de ontwikkelingen rond DORA. Dat betekent dat alle informatie die wordt gedeeld, nu of in de toekomst onjuist of onvolledig kan blijken.

Inhoud

- DORA: wat te verwachten?
- DORA en de IT-auditor.

DORA: wat te verwachten?

DORA in het kort (1/2)

Een alomvattend en sectoroverstijgend kader voor digitale operationele weerbaarheid voor:

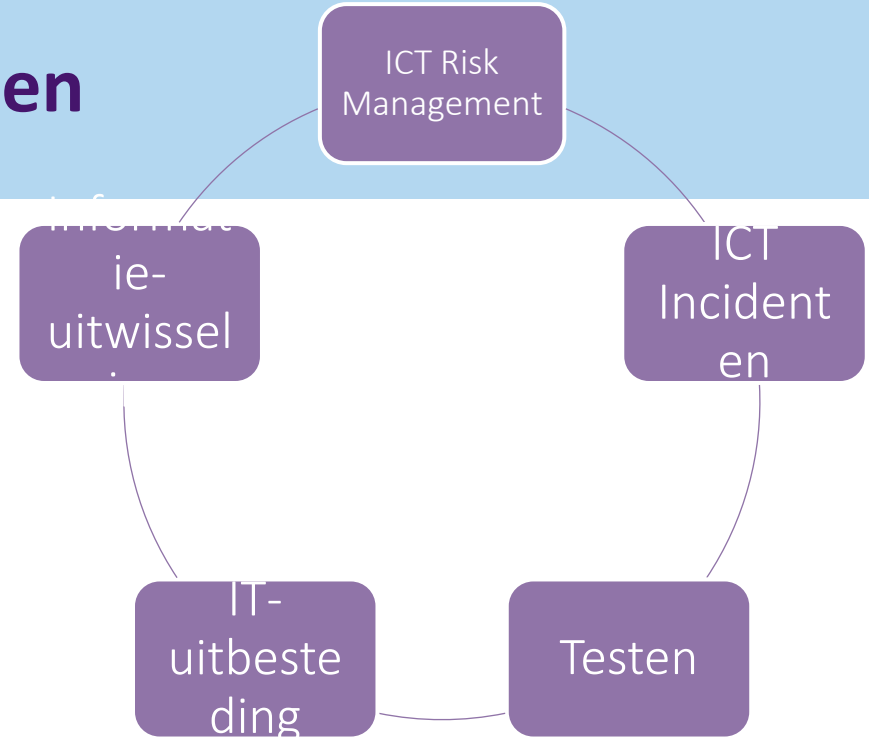
- Verdere harmonisatie van regels voor IT-beheersing binnen de financiële sector;
- Het verplicht stellen van grondige tests van IT-systemen;
- IT-incidentrapportage stroomlijnen;
- Toezichthouders meer bevoegdheden voor toezicht op IT-uitbestedingen;
- Kritieke IT-dienstverleners onder oversight plaatsen van de ESA's.

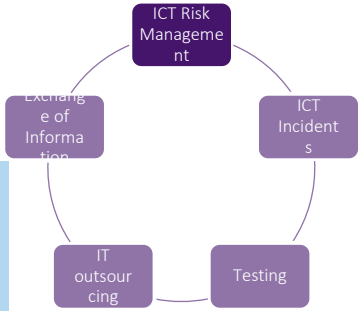
DORA in het kort (2/2)

Belangrijke kenmerken:

- Scope: partijen onder toezicht van de AFM, m.u.v. o.a. accountantsorganisaties, kleine en medium verzekeringstussenpersonen en aanbieders van krediet;
- Proportionele toepassing met uitzonderingen voor micro- en kleine ondernemingen;
- Inwerkingtreding 17-1-2023 met een implementatietermijn van 24 maanden;
- 16 aanvullende beleidsproducten (RTS, ITS).

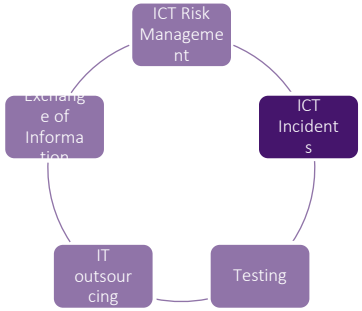
Onderwerpen





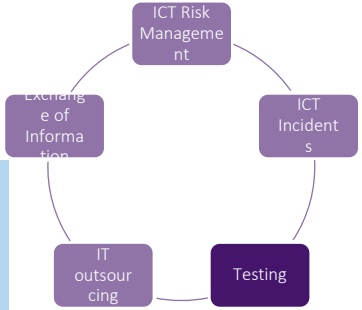
ICT Risk Management (art 5-16)

- Toewijzen van verantwoordelijkheden voor ICT Risk Management;
- ICT Business Continuity Plan implementeren en periodiek testen;
- Kennis van informatiebeveiliging op bestuursniveau.



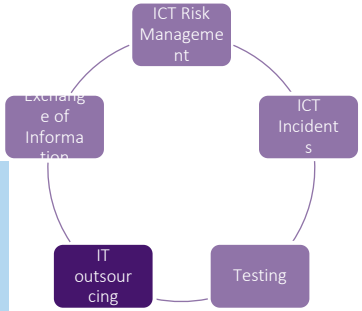
ICT-incidenten (art 15-20)

- Instellingen moeten een process inrichten voor het detecteren en afhandelen van incidenten;
- Incidenten moeten worden vastgelegd en geclassificeerd;
- Entiteiten verstrekken rapportages over significante ICT-incidenten



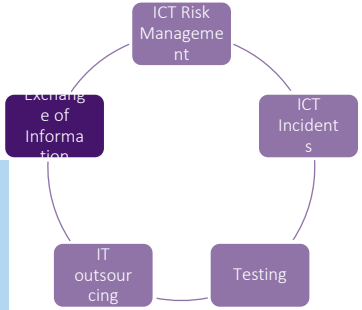
Testen (art 21-24)

- Testprogramma voor testen van cyberweerbaarheid wordt verplicht;
- TLPT-verplichting voor meest significante ondernemingen;
- In Nederland wordt TLPT ingevuld met TIBER.



IT-uitbesteding (art 25-39)

- Vaste onderdelen in overeenkomsten (risk assessments, right to audit, exit-strategieën, onderuitbesteding en meer);
- Bijhouden van een uitbestedingsregister;
- Oversight regime voor grootste IT-dienstverleners.



Informatie-uitwisseling (art 40)

- Op vrijwillige basis mogen ondernemingen informatie en inlichtingen over cyberdreigingen uitwisselen.

Toezicht op DORA

- Toezicht door AFM en DNB, naar verwachting langs de lijn van vergunningverstrekking;
- Risicogestuurd toezicht;
- TLPT-begeleiding voor TIBER.

Ontwikkeling van beleidsproducten

- Eerst batch beleidsproducten staat uit ter consultatie, waaronder RTS ICT Risk Management, Register of Information, Criteria for ICT Incidents, Policy for Outsourcing
- Ondernemingen worden uitgenodigd om te reageren op deze consultaties.

ESMA European Securities and Markets Authority

eiopa European Insurance and Occupational Pensions Authority

EBA EUROPEAN BANKING AUTHORITY

Vooruitblik

- Veel nieuwe normen, voor kleinere ondernemingen mogelijk grote ‘delta’
- Advies om tijdig te beginnen met implementatie – indien nog niet begonnen;
- Diverse beleidsproducten worden nog geconsulteerd.

DORA en de IT-auditor

Rol van audit in DORA (1/2)

- Three lines: passende scheiding en onafhankelijkheid verplicht;
- Auditors beschikken over voldoende kennis op het gebied van IT-risico's;
- IT-auditplannen moeten door bestuur worden goedgekeurd en periodiek geëvalueerd;
- Formeel follow-upproces voor auditbevindingen.

Rol van audit in DORA (2/2)

- Kader voor IT-risicobeheer wordt regelmatig geaudit;
- Verplicht right to audit (door interne of aangewezen externe auditors) in contracten met IT-dienstverleners die kritieke of belangrijke diensten ondersteunen.

Kansen voor de auditor

- Uitvoeren nulmeting (en 1-meting);
- Actief meekijken met gap-analyse en plan van aanpak DORA-implementatie.

Vragen?

PENSIOEN FEDERATIE

PF

Presentatie DORA - issues bij implementatie

26 oktober 2023 – NOREA

DORA

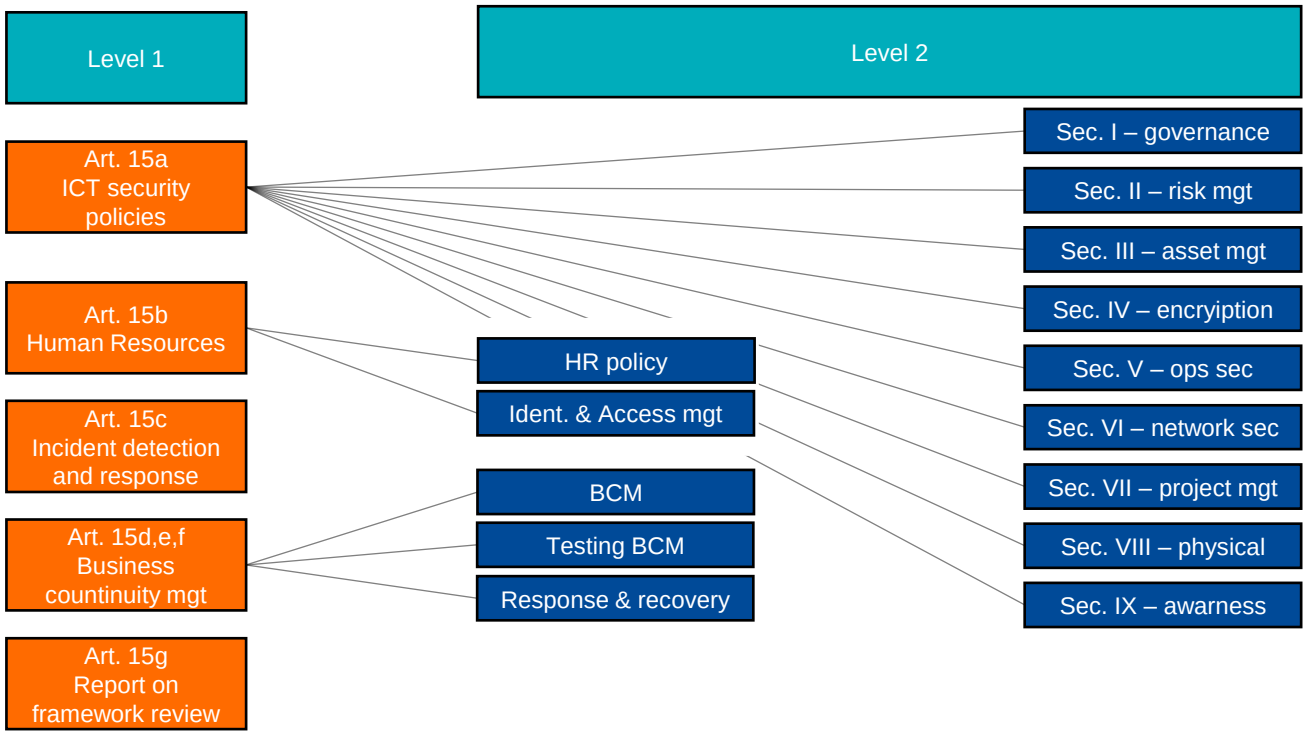
- Per januari 2023 is de Digital Operational Resilience Act (DORA) geaccordeerd en richt zich op het uniformeren en standaardiseren van wet- en regelgeving over de beheersing van ICT-risico's voor de financiële sector. Op 17 januari 2025 dient elk pensioenfonds te voldoen aan DORA-wetgeving (directe werking).

- Met DORA heeft de Europese Commissie drie hoofddoelen voor ogen:
  - Versnipperde regels ten aanzien van digitale weerbaarheid in de EU harmoniseren;
  - Een basiskader scheppen voor financiële organisaties waarvoor nog geen regelgeving is;
  - Het beter mitigeren van risico's van uitbesteding door de financiële sector aan kritieke digitale derde dienstverleners.

- DORA bestaat uit vijf pijlers:
  1. ICT-risicobeheer
  2. ICT-gerelateerde incidenten
  3. Testen van digitale weerbaarheid
  4. Beheer van ICT-risico's van derde aanbieders/Oversight
  5. Informatie-uitwisseling over cyberdreigingen en kwetsbaarheden

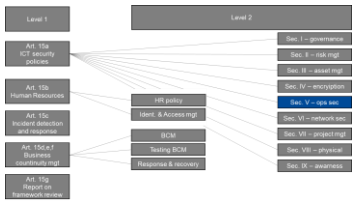
	DORA policy work	Article	Public consultation	Finalise
	Call for advice on criticality criteria and fees	31.8 | 43.2	26 May - 23 June 23	30 Sept 2023
FIRST BATCH	RTS on ICT risk management framework	15		
	RTS on simplified ICT risk management framework	16		
	RTS on criteria for the classification of ICT-related incidents	18.3	19 June - 11 Sept 23	17 Jan 2024
	ITS to establish the templates for the Register of information	28.9		
	RTS to specify the policy on ICT services performed by 3rd party	28.1		
SECOND BATCH	RTS on specifying the reporting of major ICT-related incidents	20.a		
	ITS to establish the reporting details for major ICT-related incidents	20.b		
	Guidelines on the estimation of aggregated costs/losses caused by major ICTrelated incidents	11.11		
	RTS to specify threat led penetration testing aspects	26.11	Nov/Dec 23 - TBC	17 June 2024
	RTS to specify elements when sub-contracting critical or important functions	30.5		
	GL on cooperation between ESAs and CAs regarding the structure of the oversight	32.7		
	RTS to specify information on oversight conduct	41		
	Feasibility report on single EU Hub for major ICT-related events	21	TBC	17 January 2025

RTS ICT risicomanagement framework



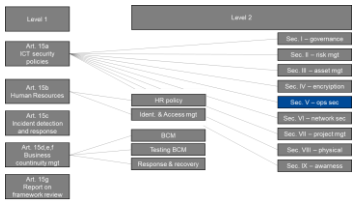
Operations security | vulnerability & patch mgt

- Art. 10 lid 2 sub c: These procedures shall:
  - Ensure that ICT third-party service providers handle any vulnerabilities related to the ICT services provided to the financial entity and report them to the financial entity. In particular, financial entities shall request that ICT third-party services providers investigate the relevant vulnerabilities, determine the root cause and implement appropriate solutions.



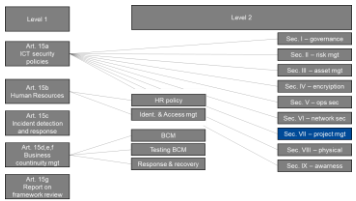
Operations security | data & system security

- Art. 11 lid 2 sub f: Data and system security procedure shall include all of the following elements related to data and ICT system security […]:
  - Requirements to secure the use of portable endpoint devices and private non-portable endpoint devices as follows:
    - the use of a centralised management solution to remotely manage the endpoint devices and remotely wipe the financial entity's data;
    - the use of security mechanisms that cannot be modified, removed or bypassed by staff members or ICT third-party service providers;
    - the authorisation to use removable data storage devices only where the residual ICT risk remains wihtin the financial entity's risk tolerance levels.



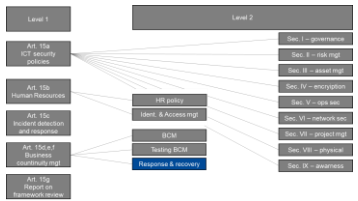
Project & change mgt | system acquisitions

- Art. 16 lid 4: Financial entities shall perform source code review covering both static and dynamic testing. The testing shall include security testing for internet-exposed systems and applications. Financial entities shall identify and analyse anomalies in the source code, adopt an action plan to adress them and monitor their implementation.



Response & recovery plans

- Art. 27 lid 2: The ICT response and recovery plans shall identify relevant scenarios […], include all of the following:
  - cyber-attacks and switchovers between the primary ICT infrastructureand the redundant capacity, backups and redundant facilities;
  - Scenarios in which the quality of the provision of a critical or important function deteriorates to an unacceptable level or fails, and duly considers the potential impact of the insolvency, or other failures, of any relevant ICT third-party service provider;
  - Partial or total failure of premises, including office and business permises, and data centres;
  - Substantial failure of ICT assets or of the communication infrastructure;
  - The non-availability of a critical number of staff or key staff members;
  - Natural disasters, pandemic situations and physical attacks, including intrusions and terrorist attacks;
  - Insider attack;
  - Political and social instability, including where relevant, in the jurisdiction from where the ICT third-party service provider provides its services and the location where the data is stored and processed;
  - Widespread power outage.



Discussievragen

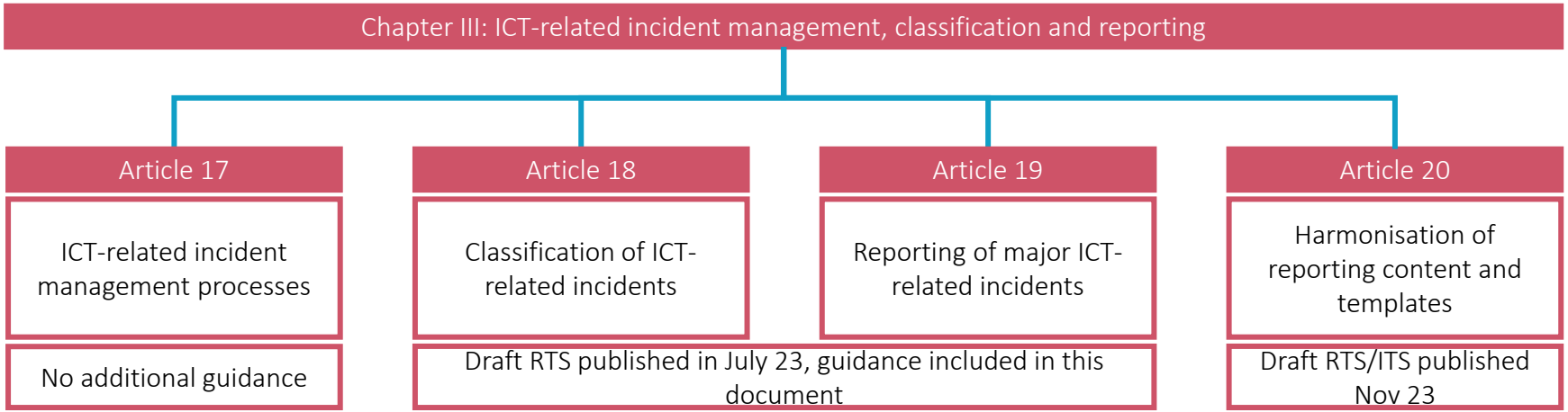
- Wanneer kun je aantonen te voldoen aan DORA?
- Wat is proportionaliteit in deze wetgeving?
- Inrichting van de three lines: niet elke bestuurder zal evenveel van IT weten en dat is goed.
- Stel gap analyse uitgevoerd, veel is nog onduidelijk/hoe te interpreteren. Houd hier rekening mee in het oordeel.
- Hoe ver gaat de audit, wanneer mag wat te verwachten zijn?

DORA Chapter III – ICT-related incident management, classification and reporting

Norea round table

DORA Chapter III – ICT-related incident management, classification and reporting

Chapter III consists of 4 articles describing the management of ICT-related incidents and the classification & reporting of major incidents

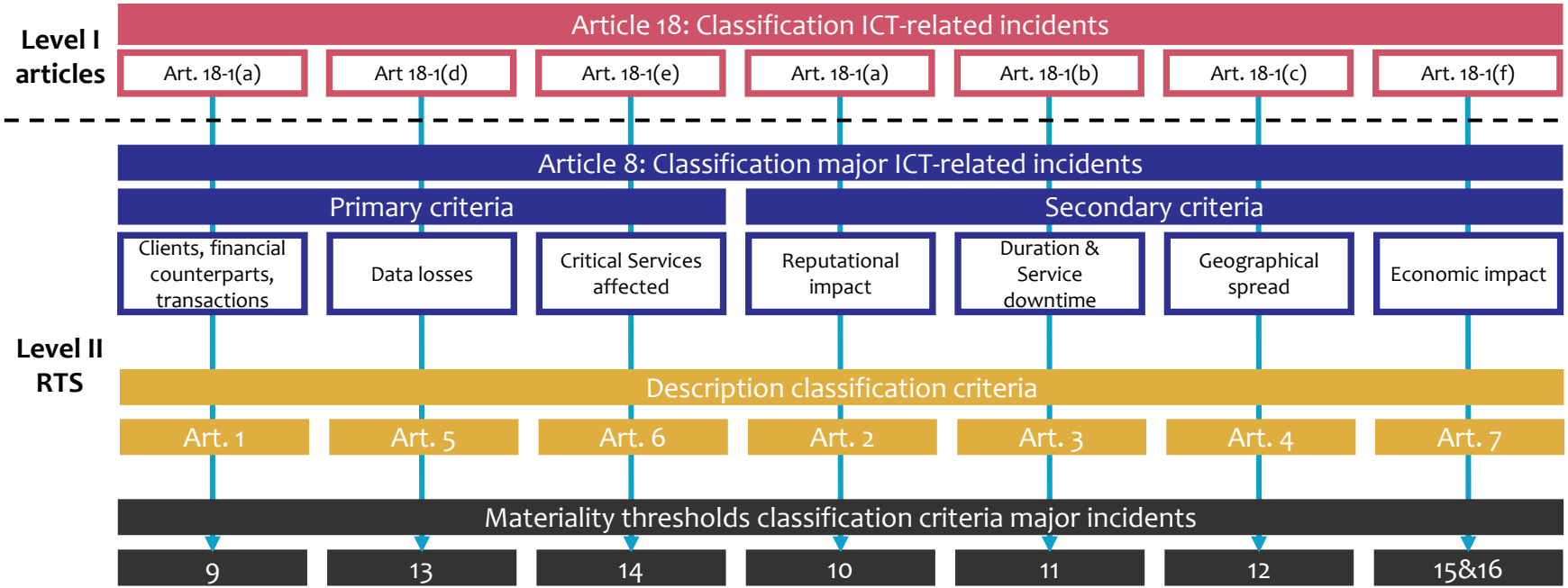


Article 17 – ICT related management process

1. Define, establish and implement an ICT-related incident management process to **detect, manage and notify ICT-related incidents**, including:
   a) Early warning indicators;
   b) Procedures to identify, track, log, categorise and classify ICT-related incidents according to their priority and severity and according to the criticality of the services impacted
   c) assigned roles and responsibilities that need to be activated for different ICT-related incident types and scenarios;
   d) Plans for communication to staff, external stakeholders and media and for notification to clients, for internal escalation procedures, including ICT-related customer complaints, as well as for the provision of information to financial entities that act as counterparts, as appropriate;
   e) At least major ICT-related incidents are reported to relevant senior management and the management body is informed of at least major ICT-related incidents, explaining the impact, response and additional controls to be established as a result of such ICT-related incidents;
   f) ICT-related incident response procedures to mitigate impacts and ensure that services become operational and secure in a timely manner.
2. **Record all ICT-related incidents** and significant cyber threats.
3. Establish appropriate procedures and processes to ensure a consistent and integrated monitoring, handling and follow-up of ICT-related incidents, to ensure that **root causes are identified, documented and addressed** in order to prevent the occurrence of such incidents.

Article 18– ICT-related incident classification major/non-major – Level I vs Level II

The majority of the Level II guidance provides further explanation on the criteria for classifying ICT-related incidents as described in article 18 DORA



Article 18- Classification criteria major ICT-related incidents

1. **ICT-related incidents** qualify as **major** and need to be reported by the financial entity to the competent authorities if they meet one of the following options:
   - I. **Two primary criteria** have been met; **or**
   - II. **One primary criterion** and **two secondary criteria** have been met.

Primary criteria:

1. 'Clients, financial counterparts and transactions' as set out in Article 1;
2. 'Data losses' as set out in Article 5; and
3. 'Critical services affected' as set out in Article 6.

Secondary criteria:

1. 'Reputational impact' as set out in Article 2;
2. 'Duration and service downtime' as set out in Article 3;
3. 'Geographical spread' as set out in Article 4; and
4. 'Economic impact' as set out in Article 7.

Article 18- Thresholds major ICT-related incidents

Each criterion has a threshold that needs to be met before the criterion becomes applicable

	Criteria	Thresholds
Primary criteria	Clients, financial counterparts transactions affected by incident	10% of clients **or** financial counterparts **or** transactions are **affected** by the ICT-related incident
	Critical services affected by the incident	The incident affected services or activities that require authorisation, or ICT services that support critical or important functions Impact on critical services that has been escalated to senior management or management body, shall be considered meeting the threshold
	Data losses	ICT-related incident has significant impact on availability, authenticity, integrity or confidentiality of critical data

Article 18- Thresholds major ICT-related incidents

Each criterion has a threshold that needs to be met before the criterion becomes applicable

	Criteria	Thresholds
Secondary criteria	(Expected) reputational impact	a) media attention; or b) complaints clients or financial counterparts; or c) Unable to meet regulatory requirements; or d) Likely to lose clients or financial counterparts with an impact on its business
	Duration & service downtime	1. the duration of the incident > 24 hours; or 2. the service downtime > 2 hours for ICT services supporting critical functions
	Geo-graphical spread	impact of the incident in at least two Member States, including on: a) The clients & financial counterparts affected; or b) Financial market infrastructures or third-party providers that may be common with other financial entities.
	Economic impact	Gross direct and indirect costs and losses incurred by the financial entity from the major incident have exceeded or are likely to exceed EUR 100,000.

Article 19– ICT-related incident reporting requirements

Key observation here is that we are still awaiting further guidance on the reporting process, to be published on Nov/Dec, which is also expected to provide more guidance on the reporting deadlines

Communication requirements	Reporting requirements	Outsourcing
Where a major ICT-related incident occurs and has an impact on the financial interests of clients, financial entities shall inform their clients about the major ICT-related incident and about the measures that have been taken to mitigate the adverse effects of such incident.	financial entities shall, within the time limits to be laid down in accordance with Article 20, first paragraph, point (a), point (ii), submit the following to the relevant competent authority: a) an initial notification; b) an intermediate report after the initial notification referred to in point (a), as soon as the status of the original incident has changed significantly or the handling of the major ICT-related incident has changed based on new information available, followed, as appropriate, by updated notifications every time a relevant status update is available, as well as upon a specific request of the competent authority; c) a final report, when the root cause analysis has been completed, regardless of whether mitigation measures have already been implemented, and when the actual impact figures are available to replace estimates.	Financial entities may outsource, in accordance with Union and national sectoral law, the reporting obligations under this Article to a third-party service provider. In case of such outsourcing, the financial entity remains fully responsible for the fulfilment of the incident reporting requirements.

Article 20: Harmonisation of reporting content and templates

Section to be finalized after RTS and ITS are published in Nov23, which should provide more details on contect of reporting format of templates and reporting timelines

Bedankt

Voor meer informatie kun je contact opnemen met:

[Kennisgroep Betalingsverkeer]
[telefoonnummer]
[norea@norea.nl]

[26 oktober 2023]