DORA voor de IT auditor: Kom maar op!

NOREA\ Kennisgroep Betalingsverkeer

13 juni 2024

NOREA

DE BEROEPSORGANISATIE VAN IT-AUDITORS

Agenda

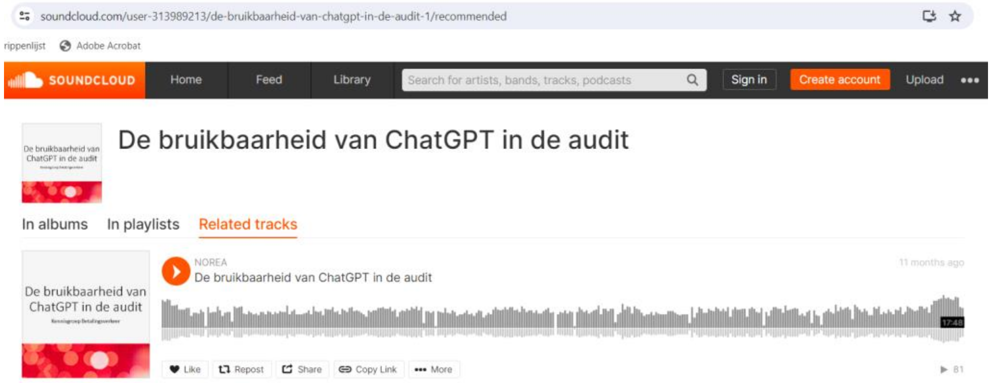
- Welkom en introductie kennisgroep Betalingsverkeer
- DORA – Digital Operational Resilience Act
- Introductie sprekers
- ‘DORA from an auditor perspective’ – Gertjan Verhage
- ‘DORA – Digital Operational resilience Testing’ – Marcel van Beek
- Afsluiting

Introductie Kennisgroep Betalingsverkeer

- Leden van de groep:
  - Wandena Birdja-Punwasi
  - Caroline Zonneveld
  - Léon Dirks
  - Mike Leeman
  - Edward van Dooren
  - Frank Waatjes
- De Kennisgroep Betalingsverkeer houdt zich bezig met totstandbrenging van relevante producten, publicaties en seminars op het gebied van betalingsverkeer. Zie ook de video en/of Twitteraccount: @PaymentFriends.
- https://www.norea.nl/organisatie/kennis-en-werkgroepen/kennisgroep-betalingsverkeer

Introductie Kennisgroep Betalingsverkeer

- Publicaties
  Actuele ontwikkelingen en risico's in het betalingsverkeer
- Handreiking auditaanpak PSD2 (update 2023) en Worksheet
- Update PSD2, webinar oktober 2021
- Interview normenkader PSD2, 202
- Presentation Guidance Payment Service Directive 2 (update 2023)


soundcloud.com/user-313989213/de-bruikbaarheid-van-chatgpt-in-de-audit-1/recommended

De bruikbaarheid van ChatGPT in de audit

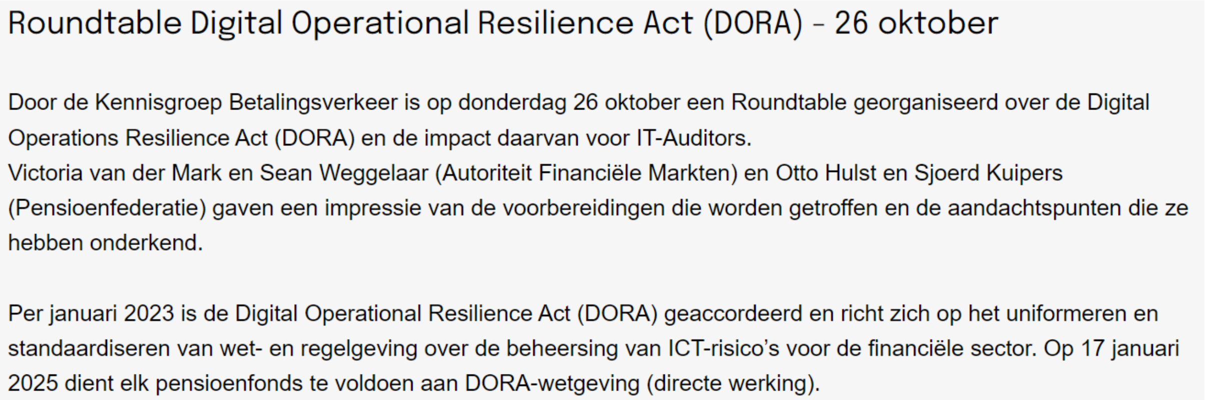
NOREA

De bruikbaarheid van ChatGPT in de audit

11 months ago

DORA

- DORA
  - Eerdere DORA presentatie:



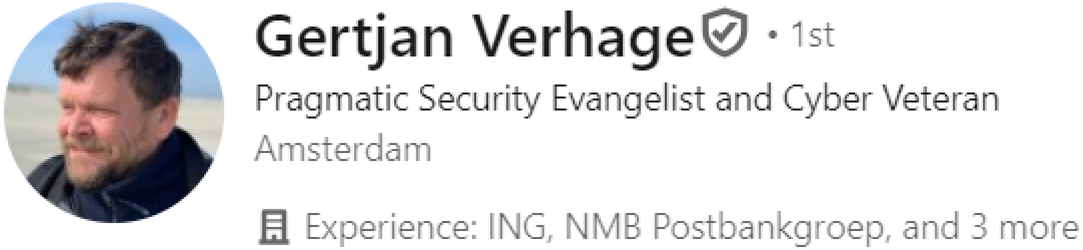
Roundtable Digital Operational Resilience Act (DORA) - 26 oktober

Door de Kennisgroep Betalingsverkeer is op donderdag 26 oktober een Roundtable georganiseerd over de Digital Operations Resilience Act (DORA) en de impact daarvan voor IT-Auditors.
Victoria van der Mark en Sean Weggelaar (Autoriteit Financiële Markten) en Otto Hulst en Sjoerd Kuipers (Pensioenfederatie) gaven een impressie van de voorbereidingen die worden getroffen en de aandachtspunten die ze hebben onderkend.

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).

  - DORA is een EU-verordening gericht op cyberweerbaarheid. Financiële instellingen hebben tot 17 januari 2025 de tijd om aan DORA te voldoen. Vanaf dan moeten de beheersmaatregelen geïmplementeerd zijn. Vandaag worden de volgende onderwerpen vanuit een IT auditor perspectief besproken:
    - ICT-risicobeheer
    - ICT-gerelateerde incidenten
    - testen van digitale operationele veerkracht
    - beheer van ICT-risico van derde aanbieders
    - informatie-uitwisseling

Introductie sprekers

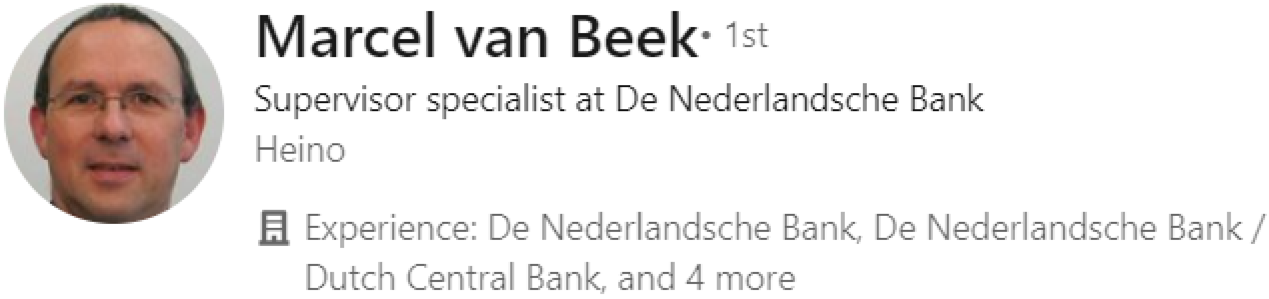


Gertjan Verhage • 1st

Pragmatic Security Evangelist and Cyber Veteran

Amsterdam

Experience: ING, NMB Postbankgroep, and 3 more



Marcel van Beek• 1st

Supervisor specialist at De Nederlandsche Bank

Heino

Experience: De Nederlandsche Bank, De Nederlandsche Bank / Dutch Central Bank, and 4 more

Bedankt

Voor meer informatie kun je contact opnemen met:

Kennisgroep Betalingsverkeer
norea@norea.nl

13 juni 2024

DORA from an auditor perspective

Gertjan Verhage
13 June 2024

DRAFT 0.1

DORA

Digital
Operational
Resilience
Act

Who am I?

Gertjan Verhage
Pragmatic Security Evangelist and Cyber veteran

35+ years of experience in IT, IT Security, Information Security, IT Risk Management

Currently employed as Sr. Consultant Information Security with focus on horizon scanning and advocacy on **law and regulation in IT Risk and Cybersecurity**

Hobby: (competitive) sailing and travel

Agenda

Gertjan Verhage

1. Short introduction on DORA
2. Third party Risk Management
3. DORA Major incident reporting
4. DORA register of information

Marcel van Beek

5. Threat Led Penetration Testing
6. Crises management

Introduction DORA | DORA context

The Digital Operational Resilience Act (DORA) is the regulation that aims to strengthen the information and communication technology (ICT) security of financial entities in the European Union (EU).

On 24 September 2020, the European Commission (EC) published proposals on digital operational resilience, comprising a draft regulation (DORA) alongside a proposed directive. DORA has been formally adopted, and the regulation entered into force on **16 January 2023** and will apply as of **17 January 2025.**

DORA provides the financial sector the opportunity to further improve and broaden operational resilience. Harmonizing IT cybersecurity requirements, coupled with a **'lex specialis'** approach, aims to streamline and prevent the duplication of efforts.

Context

1. Information and communication technology (ICT) supports complex systems used for everyday activities of the financial sector. **The extended use of ICT systems increases the efficiencies of internal process and the user experience for the customers; however, it also introduces risks and vulnerabilities, which may make financial entities expose to cyber-attacks or incidents.** If not managed properly, ICT risks could lead to the disruptions of financial services that are often offered across borders and can have far-reaching effects on other companies, sectors, or even the rest of the economy. **The risk of such cross-border and cross-sectoral disruptions highlights the importance of digital operational resilience of the financial sector**.
2. **As a measure to enhance the overall digital operational resilience of the EU financial sector Digital Operational Resilience Act (DORA) was published** in the Official Journal of the European Union. DORA brings harmonisation of the rules relating to operational resilience for the financial sector through DORA pillars **covering important topics such as:**
    - **ICT risk management;**
    - **ICT incident management and reporting;**
    - **testing of the operational resilience of ICT systems;**
    - **management of ICT third party risks**
    - **information sharing**
3. To operationalise the application, DORA mandates the European Supervisory Authorities (ESAs) to prepare jointly, through the Joint Committee (JC), a **set of policy products – Regulatory Technical Standards (RTS)** & implementing technical standards (ITS) **-** with two main submission deadlines. These technical standards aim to ensure a consistent and harmonised legal framework in DORA pillars. Before submission the draft version will be shared to allow consultation.

Introduction DORA | 5 Dora pillars introduction (1/2)

DORA introduces requirements across 5 pillars: Management of ICT risks, Threats and incident reporting, Digital operational resilience test, Managing 3rd - party risk management and Information sharing

		1. Management of ICT risk	2. Classification and reporting of threats and incidents	3. Digital operational resilience test
DORA Pillar description		Article: 5-16 **DORA sets out key principles around internal controls and governance structures**	Article: 17-23 **DORA proposes to harmonise incident reporting processes and documentation**	Article: 24-27 **DORA requires financial entities to periodically test their ICT risk management framework**
		• Set-up and maintain resilient ICT systems and tools that minimize the impact of ICT risk. • All sources of ICT risks should be continuously identified to set-up protection and prevention measures. • A prompt detection of anomalous activities should be established. • Dedicated and comprehensive business continuity policies and disaster and recovery plans should be in place, ensuring a prompt recovery after an ICT-related incident. • Establish mechanisms to learn and evolve both from external events as well as the entity's own ICT incidents.	• Establish and implement a management process to monitor and log ICT-related incidents. • Classify the incident according to the criteria detailed in the regulation and further developed by the ESAs. • Ensuring the reporting of incidents to the relevant authorities using a common template.. • Submit initial, intermediate and final reports on ICT-related incidents to NCA's and inform the firm's users and clients.	• Elements within the ICT risk management framework should be periodically tested for preparedness. • Any weaknesses, deficiencies or gaps must be identified and promptly eliminated or mitigated with the implementation of counteractive measures. • Digital operational resilience testing requirements must be proportionate to the entities' size, business and risk profiles. • Conduct Threat Led Penetration Testing (TLTP), also known as a Red / Purple Team Assessment, to address higher levels of risk exposure.
Scope of RTS's	RTS batch 1	• RTS on **ICT risk management framework** (Art.15). • RTS on **simplified ICT risk management** framework	• RTS on criteria for the **classification of ICT-related incidents** (Art. 18.3)	n/a
	RTS batch 2	• Guidelines on the estimation of **aggregated annual costs/losses caused by major ICT incidents** (Art. 11.12)	• RTS on **specifying the reporting of major ICT-related incidents** (Art. 20.a) • ITS to establish the **reporting details for major ICT-related incidents** (Art. 20.b)	• RTS to specify **threat led penetration testing aspects** (Art. 26.11)

Not final yet

Introduction DORA | 5 Dora pillars introduction (2/2)

DORA introduces requirements across 5 pillars: Management of ICT risks, Threats and incident reporting, Digital operational resilience test, Managing 3rd - party risk management and Information sharing

		4. Managing third-party risk	5. Information sharing
DORA Pillar description		Article: 28-44 **DORA requires financial entities to monitor risks in connection with their use of ICT services provided by third parties**	Article: 45 **DORA facilitates arrangements between financial entities to exchange cyber threat information and intelligence amongst themselves**
		• Ensure sound monitoring of risks emanating from the reliance on ICT third-party providers. • Harmonising key elements of the service and relationship with ICT third-party providers to enable a 'complete' monitoring. • Ensure that the contracts with the ICT third-party providers contain all the necessary monitoring and accessibility details such as a full service ldescription, indication of locations where data is being processed,.. • Promote convergence on supervisory approaches on the ICT third-party risks by subjecting the service providers to a Union Oversight Framework.	• The guidelines encourage collaboration among trusted communities of other financial entities. This collaboration will: → enhance the digital operational resilience of financial entities → raise awareness on ICT risks → minimise ICT threats' ability to spread → support entities' defensive and detection techniques, mitigation strategies or response and recovery stages. • Financial entities are encouraged to exchange amongst themselves cyber threat information and intelligence through arrangements that protect the potentially sensitive nature of the information shared.
Scope of RTS's	RTS batch 1	• RTS to specify the **policy on ICT services** (Art. 29.10) • ITS to establish the **templates for the Register of information** (Art. 29.9)	n/a
	RTS batch 2	• RTS to **specify elements when sub-contracting critical or important functions** (Art. 30.5) • Guidelines on cooperation between ESAs and CAs regarding the structure of the oversight* • RTS to specify information on oversight conduct	n/a

Not final yet

Introduction DORA | Generic auditors' perspective

- For Audit functions, operational resilience assurance has already been incorporated into audit programs. Still, DORA and its associated international regulatory efforts do **require targeted reviews and enhancements of audit plans and work programs**
- Implementing DORA is mainly the responsibility of the first and second line. Internal audit functions will need to start early to assess and prepare **changes to their audit programs and practices** to meet DORA requirements as well as to monitor the progress of implementing DORA.

- To prepare for DORA, DNB released an update to the **DNB Information Security Good Practice** on December 19, 2023. However,
  - this version of the DNB Good Practice does **not (yet) include all the requirements** from DORA.
  - the scope of DORA is **much more detailed** and stringent than the DNB Good Practice IB.

DORA explicitly mentions the role of internal audit in promoting operational resilience (Article 6, paragraph 4/6, DORA):

- *6.4 Financial entities, other than microenterprises, shall assign the responsibility for managing and overseeing ICT risk to a control function and ensure an appropriate level of independence of such control function in order to avoid conflicts of interest. Financial entities shall ensure appropriate segregation and independence of ICT risk management functions, control functions, and* ***internal audit functions****, according to* ***the three lines of defence model****, or an internal risk management and control model.*
- *6.6 The* ***ICT risk management framework*** *of financial entities, other than microenterprises, shall be* ***subject to internal audit by auditors*** *on a regular basis in line with the financial entities' audit plan. Those auditors shall possess sufficient knowledge, skills and expertise in ICT risk, as well as appropriate independence. The frequency and focus of ICT audits shall be commensurate to the ICT risk of the financial entity.*

ICT Third Party & Intra group Party Management | Management framework

First line perspective

DORA reference

DORA Art. 28(2): As part of their ICT risk management framework, financial entities.. shall adopt, and regularly review a strategy on ICT third-party risk..

The strategy on ICT third-party risk shall include a policy on the use of ICT services supporting critical or important functions.

Main Objective

The main objective on the use of ICT services (particularly for Critical or Important functions) is to **establish a clear framework to ensure the integrity, security, and reliability of ICT services, enabling financial entities to effectively mitigate risks and maintain the operational resilience of their critical functions.**

Scope and Definition

A Critical Important function

"a function, the **disruption** of which would materially **impair** the **financial performance** of a financial entity, or the soundness or **continuity** of its services and activities, or the discontinued, defective or failed performance of that function would **materially impair the continuing compliance of a financial entity** with the conditions and obligations of its authorization, or with its other obligations under applicable financial services law"

B ICT Third Party Provider

- **ICT third-party provider**: Any entity that offers services related to Information and Communication Technologies (ICT), including the provision, maintenance, or operation of hardware, software, networks, or cloud-based solutions.
- **Critical ICT third-party providers:** Any entity that delivers services critical to the functioning of organizations, encompassing telecommunications, internet services, hosting, data processing, software development, and support activities.

Framework

1 Overall Risk Profile

- The **type of ICT service, location** of the ICT service provider, **data and their nature**
- The potential **impact** of a **disruption of the ICT service**
- The **concentration (including subcontracting)** and **transferability** of the ICT service

2 Governance

- Contractual arrangements are consistent with **ICT Risk Management framework, BCM, incident reporting requirements, Information security**
- **Framework is consistently implemented** in subsidiaries and periodically reviewed
- **Roles and Responsibilities, procedures clearly defined**; Management involved in decision-making

3 Risk Assessment, Conflict of Interest

- Perform **risk assessment before** entering a contract
- Assess **concentration risks & subcontracting risks**
- Define measures to identify, prevent and manage **conflict of Interest**

4 Due Diligence

- Define an **appropriate and proportional process to assess vendors**
- Assess **data transfer and its risks** for each **ICT service provider** and **subcontractor**

5 Contract Remediation

- Include **relevant contractual clauses** including access to information, audits and testing rights
- **Periodically review contracts** to ensure compliance with defined IT security clauses

6 Ongoing Monitoring

- Define **measures** and **key indicators** to monitor **performance and risks**
- Define **measures to adopt contingency plans in case of shortcoming** of the ICT service provider

7 Exit and Termination

- Define and document **exit plan, exit strategy** and **termination process**
- **Test** and **review the exit & termination plans** periodically

ICT Third Party & Intra group Party Management | Management framework

Auditors perspective

Input for the audit plan:

- **Business as usual**: Audit first and second line activities, including al their new DORA related obligations.
- DORA art 28.6 *In **exercising access, inspection and audit rights over the ICT third-party service provider**, financial entities shall, on the basis of a risk-based approach, pre-determine the **frequency of audits and inspections** as well as the areas to be audited through adhering to commonly accepted audit standards in line with any supervisory instruction on the use and incorporation of such audit standards.*
- DORA art 5.2.f The management body approve and periodically review the financial entity's ICT internal audit plans, ICT audits and material modifications to them
- Internal auditor should **align**, next to first line assessments, with the **new critical TTP lead overseer** on their scope and approach to identify potential **overlaps or blind spots** in their own audit plans and work programs.

Contract

- The **outsourcing contract** should clearly specify that the institution, its internal audit function, and the competent authorities and resolution authorities have the **right to inspect and audit the CSP**.[1 and DORA 30.3.e] Contracts should include details of how the **cost of performing on-site audits is calculated**, ideally including a breakdown and indicating the maximum cost.[1]

Audit skills and knowledge

- *Where contractual arrangements concluded with ICT third-party service providers on the use of ICT services entail high technical complexity, the financial entity shall verify **that auditors, whether internal or external, or a pool of auditors, possess appropriate skills and knowledge** to effectively perform the relevant audits and assessments [*DORA art 28.6]
- That **expertise needs to be updated frequently** given the fast pace of technological progress. [1]

Joint audit

- With cloud infrastructure and services becoming increasingly complex, there is an increased need to **pool expertise and resources** given the skills and resources required for audits and the costs involved.[1]
- It is good practice for institutions to work together to audit a CSP, putting together a joint inspection team containing **at least one technical expert from each institution**. [1]
- The inspection plan could be agreed by the institutions concerned **on a consensual basis**. If, during such a joint audit, specific issues are only relevant to a single institution, institutions should **have the ability to follow up individually with the CSP** on a bilateral basis. To prevent blind spots in the conduct of audits, leadership of those inspection teams should **rotate among the supervised entities involved, changing every year**.[1]

ICT Third Party & Intra group Party Management | Management framework

Auditors perspective

Risk assessment

- An institution's internal audit function should ensure that **risk assessments are not based solely on narratives and certifications provided by the CSP** without independent assessments/reviews and the incorporation of input provided by third parties (e.g. security analysts). [1]

Audit

- The ECB understands for the purposes of compliance with Article 6(6) of DORA, the **internal audit functions** of the institutions should **regularly review** the risks stemming from the use of a CSP's cloud services. [1]
- That review should cover, among other things, [1]:
  - adequacy of the application of internal guidelines,
  - the appropriateness of the risk assessment conducted and
  - the quality of the provider's management
  - increased provider lock-in,
  - concentration of provided functions and
  - response and recovery plans (DORA Art 11.3)
  - less predictable costs,
  - aspects of data residency
  - increased difficulty of auditing,
  - lack of transparency regarding the use of sub-providers,

[1] Draft ECB Guide on outsourcing cloud services to cloud service providers

DORA Major Incident Reporting | Immediate Regulatory Reporting

First line perspective

Main Objective

Reporting obligations:

- Report major ICT related incidents to the **relevant competent authority** and, within the time limits prescribed, submit an initial notification, an intermediate report and a final report to the relevant competent authority. (Art19.4 DORA)
- Report Recurring incidents that individually do not constitute a major incident as a major incident, if combined the thresholds are met, to the relevant competent authority when monthly analysed over the past 6 months. (Article 15 Final report on the criteria for the classification of ICT related incidents)

Timelines of initial, intermediate and final report are like PSD/2 timelines

and

- Financial entities, [..] shall report to the competent authorities, upon their request, an estimation of aggregated annual costs and losses caused by major ICT-related incidents. (Art 11.10 DORA)
- Where a major ICT-related incident occurs and has an impact on the financial interests of clients, financial entities shall, without undue delay as soon as they become aware of it, 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. (Art 19.3 DORA)

Definition

An incident shall be considered a DORA major ICT related incident where:

1) it has had any **impact** on critical or important functions

and

2) where **one** of the following is met:

a) any successful, malicious and unauthorised access occurs to network and information systems, which **may** result to data losses,

or

b) **two or more** materiality criteria have been met on

i. Clients, financial counterparts and transactions
ii. Reputational impact
iii. Duration and service downtime
iv. Geographical spread
v. Data losses
vi. Economic impact

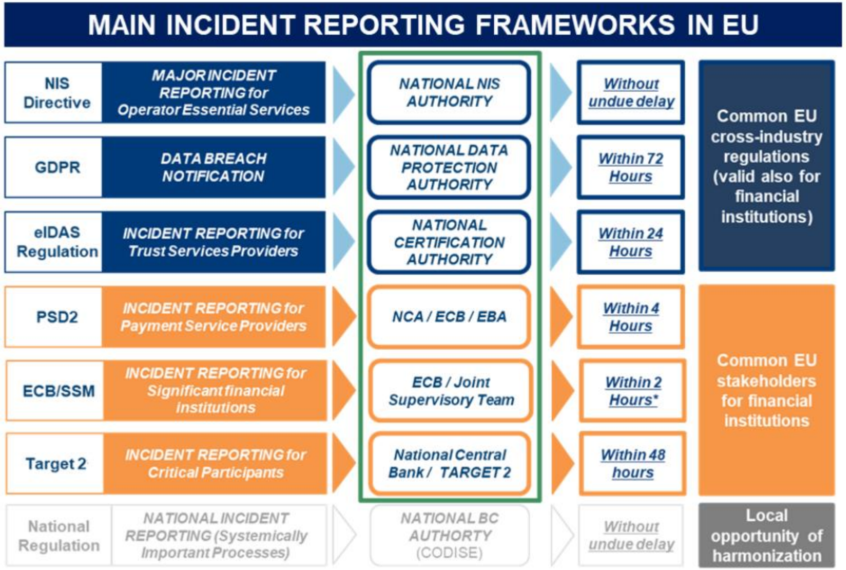
Reporting data points	Mandatory fields	Conditional fields
General information	10	8
Initial notification	9	8
Intermediate report	15	24
Final report	12	15
TOTAL	46	55

- The **materiality requirements as well as cost –estimates** are prescribed in detail in DORA RTS specifying the criteria for the classification of ICT-related incidents

DORA Major Incident Reporting | Immediate Regulatory Reporting

Auditors perspective

- DORA is **added to existing regulatory reporting obligations** (where applicable per financial entity) for **immediate regulatory incident reporting**, like
  - ECB Significant Event Reporting
  - ECB Significant Cyber Incident Reporting
  - EBA/PSD2 Major Incident Reporting (Most likely to be replaced by DORA)
  - SEPA/EPC Major Incident Reporting,
  - NIS1 Reporting (DORA is a “lex specialis” over NIS2)
- They all have their own reporting thresholds, timelines and formats, like DORA has.
- limited impact for Internal Audit, just another added quality criterium during the fieldwork



MAIN INCIDENT REPORTING FRAMEWORKS IN EU

NIS Directive	MAJOR INCIDENT REPORTING for Operator Essential Services	NATIONAL NIS AUTHORITY	Without undue delay	Common EU cross-industry regulations (valid also for financial institutions)
GDPR	DATA BREACH NOTIFICATION	NATIONAL DATA PROTECTION AUTHORITY	Within 72 Hours	
eIDAS Regulation	INCIDENT REPORTING for Trust Services Providers	NATIONAL CERTIFICATION AUTHORITY	Within 24 Hours	
PSD2	INCIDENT REPORTING for Payment Service Providers	NCA / ECB / EBA	Within 4 Hours	Common EU stakeholders for financial institutions
ECB/SSM	INCIDENT REPORTING for Significant financial institutions	ECB / Joint Supervisory Team	Within 2 Hours*	
Target 2	INCIDENT REPORTING for Critical Participants	National Central Bank / TARGET 2	Within 48 hours	
National Regulation	NATIONAL INCIDENT REPORTING (Systemically Important Processes)	NATIONAL BC AUTHORTY (CODISE)	Without undue delay	Local opportunity of harmonization

DORA register of information | arrangements with ICT third-party providers

First line perspective

DORA requires financial entities will need to have a comprehensive register of information of all their contractual arrangements with ICT third-party providers available at entity, sub-consolidated and consolidated levels (Article 28(3) starting from 17 January 2025.

The registers will serve for

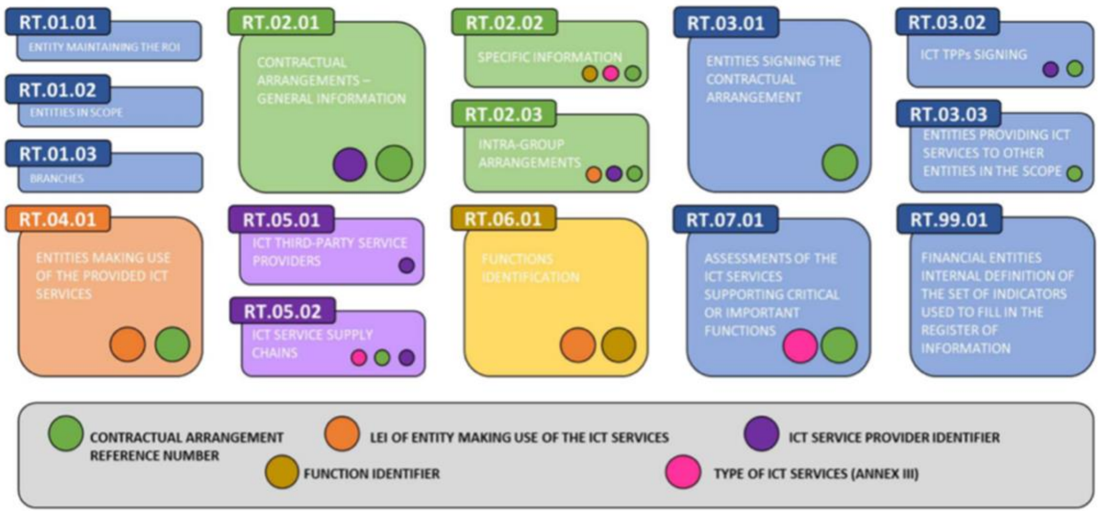
(1) financial entities to monitor their ICT third-party risk,

(2) the EU competent authorities to supervise ICT and third-party risk management at the financial entities and

(3) the ESAs to designate the critical ICT third-party service provides (CTPP) which will be subject to an EU-level oversight.

The content of those registers of information is specified in a draft ITS developed by the ESAs which is in the process of being adopted by the European Commission.

To help financial entities to be ready with their preparations, the ESAs and competent authorities will carry out a dry run on a best-efforts basis in mid-2024.



RT.01.01 ENTITY MAINTAINING THE ROI

RT.01.02 ENTITIES IN SCOPE

RT.01.03 BRANCHES

RT.02.01 CONTRACTUAL ARRANGEMENTS – GENERAL INFORMATION

RT.02.02 SPECIFIC INFORMATION

RT.02.03 INTRA-GROUP ARRANGEMENTS

RT.03.01 ENTITIES SIGNING THE CONTRACTUAL ARRANGEMENT

RT.03.02 ICT TPPs SIGNING

RT.03.03 ENTITIES PROVIDING ICT SERVICES TO OTHER ENTITIES IN THE SCOPE

RT.04.01 ENTITIES MAKING USE OF THE PROVIDED ICT SERVICES

RT.05.01 ICT THIRD-PARTY SERVICE PROVIDERS

RT.05.02 ICT SERVICE SUPPLY CHAINS

RT.06.01 FUNCTIONS IDENTIFICATION

RT.07.01 ASSESSMENTS OF THE ICT SERVICES SUPPORTING CRITICAL OR IMPORTANT FUNCTIONS

RT.99.01 FINANCIAL ENTITIES INTERNAL DEFINITION OF THE SET OF INDICATORS USED TO FILL IN THE REGISTER OF INFORMATION

● CONTRACTUAL ARRANGEMENT REFERENCE NUMBER

● LEI OF ENTITY MAKING USE OF THE ICT SERVICES

● ICT SERVICE PROVIDER IDENTIFIER

● FUNCTION IDENTIFIER

● TYPE OF ICT SERVICES (ANNEX III)

Attention points:

- Relation third party contracts to Critical Important Functions (DORA art 8)
- Classification of the service provider as a "ICT Service Provider"
  - When is a service an ICT service
- Supply chains 4th etc parties and Intragroup services
- Anticipation of remaining regulatory technical standards
- Timeline

Follow us

- ing.com
- ingwb.com
- @ING_News
- Facebook.com/ING
- LinkedIn.com/company/ING
- YouTube.com/ING
- SlideShare.net/ING
- Flickr.com/INGGroup
- Medium.com/ing-blog

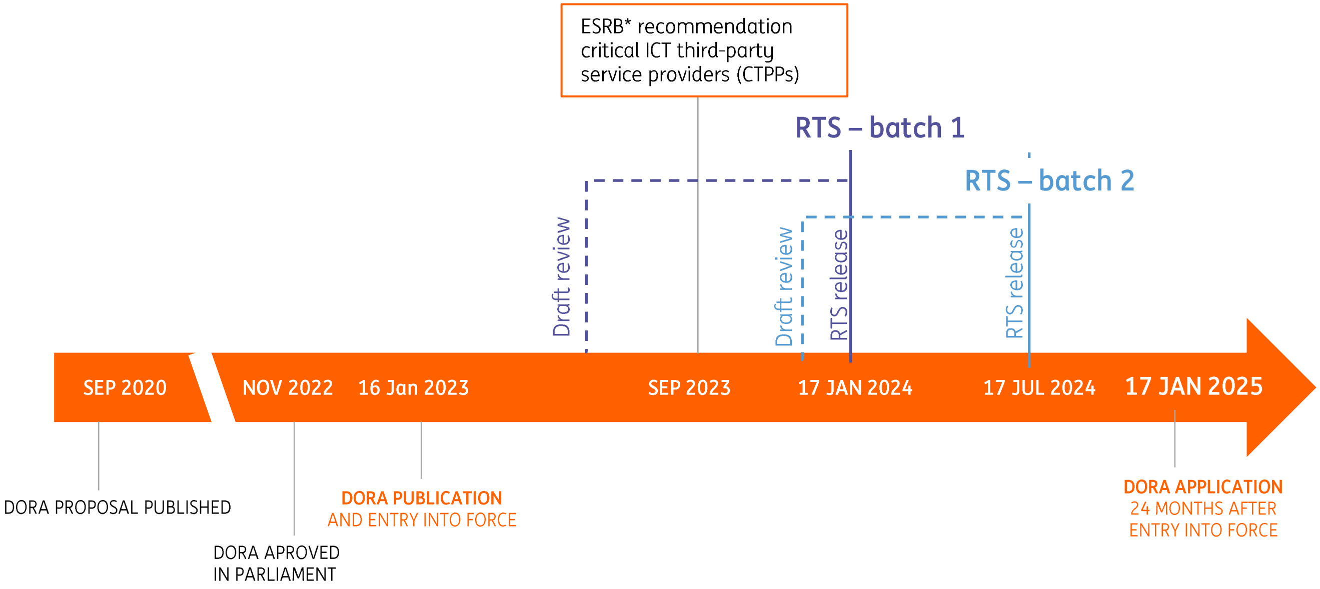
..or mail to Gertjan.Verhage@ING.com

About DORA | Timelines

DORA requirements need to be implemented before 17/01/2025, while RTS's* will be created by ESA's* along the way

DORA timelines:

1. DORA has been formally adopted by the European Parliament on 10/11/2022 and published on 16/01/2023.
2. **Entities have to implement** the DORA requirements **before 17/01/2025 (DORA application date).**
3. **Regulatory Technical Standards (RTS*)** will be created by ESA's* along the way (releases **17/01/2024 and** exp. **17/07/2024)**


ESRB* recommendation critical ICT third-party service providers (CTPPs)
RTS – batch 1
RTS – batch 2
Draft review
Draft review
RTS release
RTS release
SEP 2020
NOV 2022
16 Jan 2023
SEP 2023
17 JAN 2024
17 JUL 2024
17 JAN 2025
DORA PROPOSAL PUBLISHED
DORA APROVED IN PARLIAMENT
DORA PUBLICATION AND ENTRY INTO FORCE
DORA APPLICATION 24 MONTHS AFTER ENTRY INTO FORCE

*** Legend:** RTS - Regulatory Technical Standards | ITS - Implementing Technical Standards | DA - Delegated Acts | ESRB - European Systemic Risk Board | ESA - European Supervisory Authority

DORA – Digital Operational resilience Testing

Norea 13 juni 2024

DeNederlandscheBank

EUROSYSTEEM

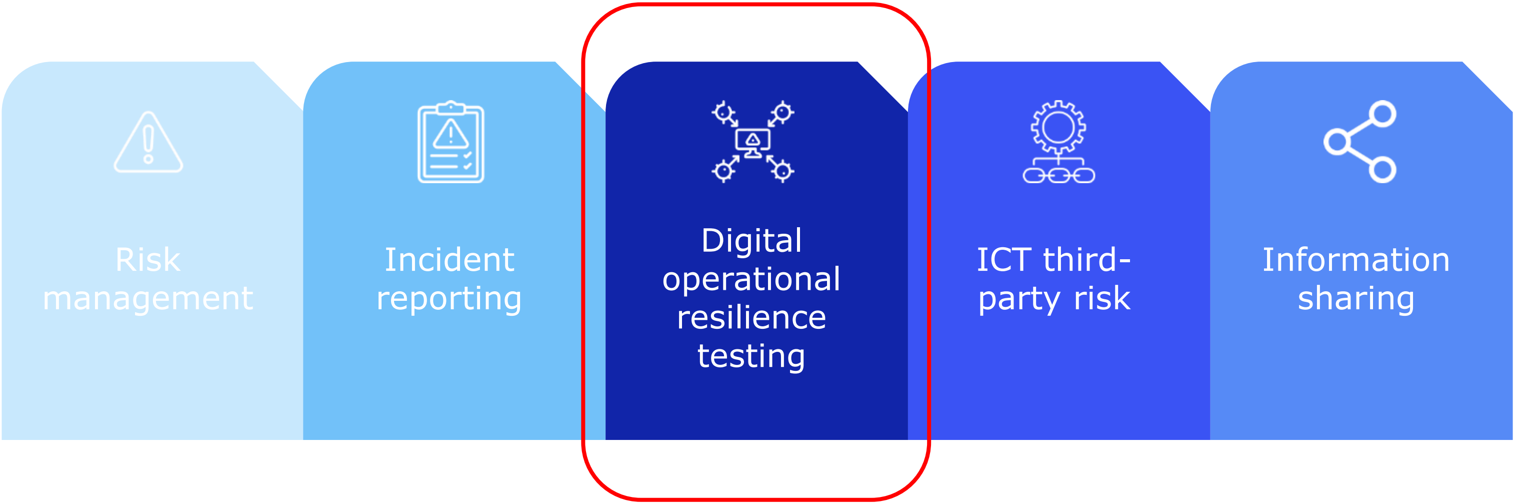
Background

DORA is part of a larger batch of EU security legislation

To increase the digital operational resilience of the financial sector

And harmonize existing provisions

DORA 5 pillars



Risk management

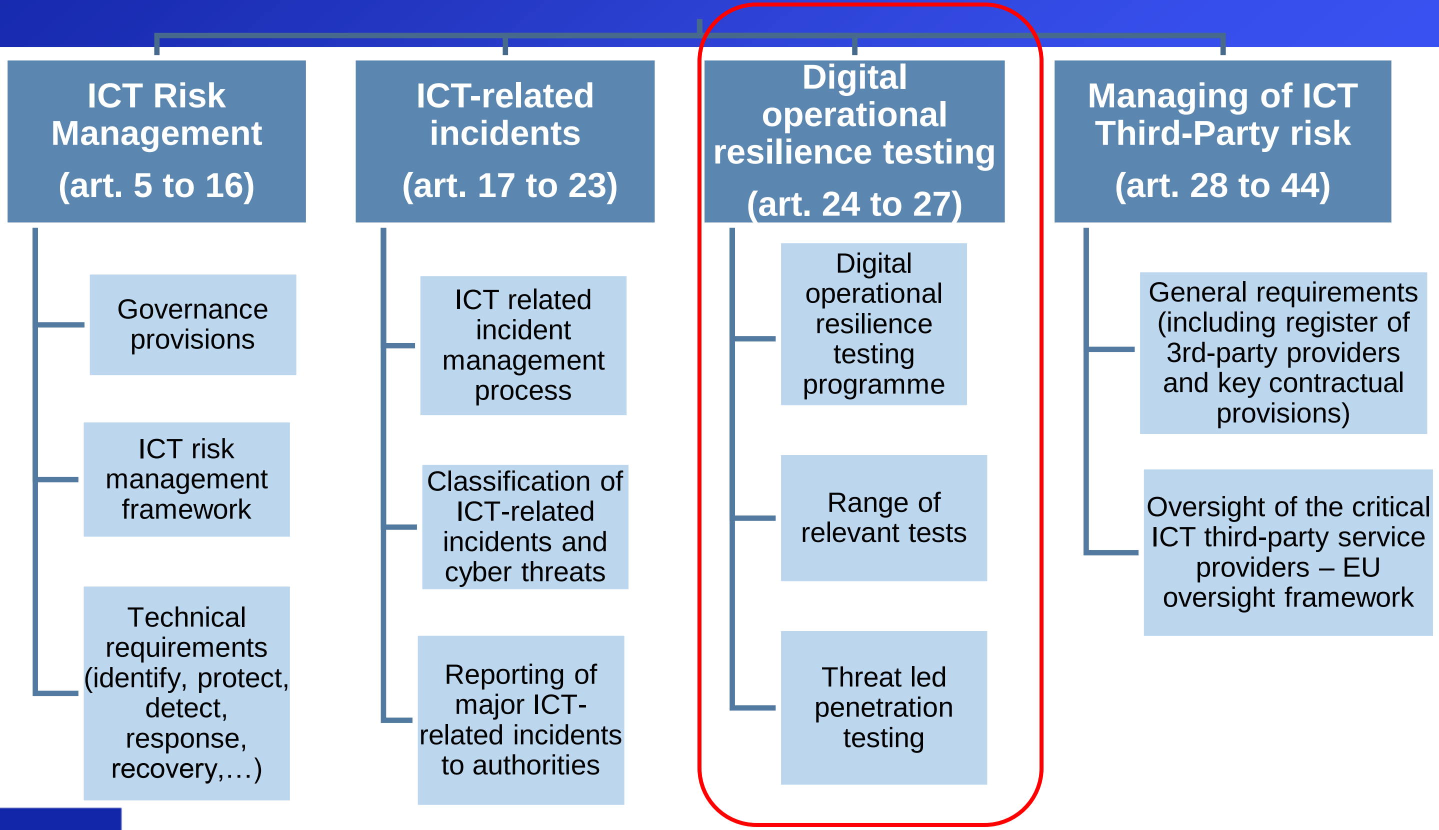
Incident reporting

Digital operational resilience testing

ICT third-party risk

Information sharing

DORA



ICT Risk Management
(art. 5 to 16)

- Governance provisions
- ICT risk management framework
- Technical requirements (identify, protect, detect, response, recovery,…)

ICT-related incidents
(art. 17 to 23)

- ICT related incident management process
- Classification of ICT-related incidents and cyber threats
- Reporting of major ICT-related incidents to authorities

Digital operational resilience testing
(art. 24 to 27)

- Digital operational resilience testing programme
- Range of relevant tests
- Threat led penetration testing

Managing of ICT Third-Party risk
(art. 28 to 44)

- General requirements (including register of 3rd-party providers and key contractual provisions)
- Oversight of the critical ICT third-party service providers – EU oversight framework

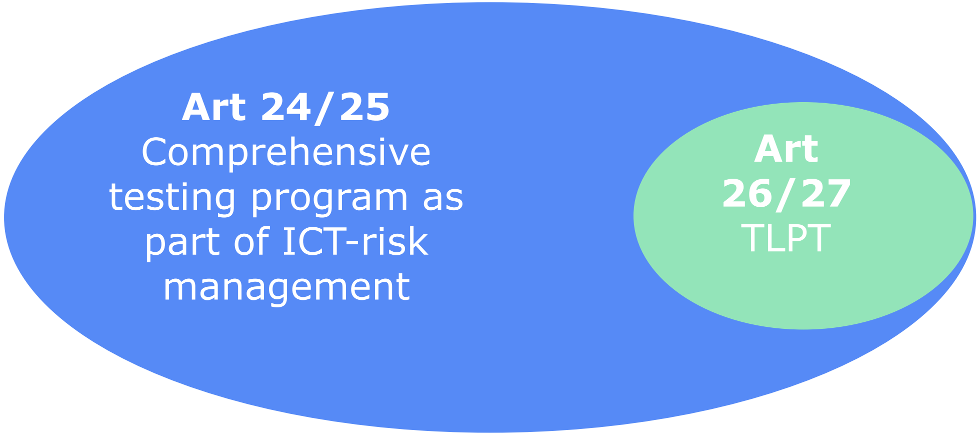
DORA – digital operational resilience testing

1 **Artikel 24/25**: related to testing Digital Operational Resilience

All financial institutions in scope of DORA

2 **Artikel 26/27**: Threat-Led Penetration Testing (TLPT)

Selected group of institutions


Art 24/25
Comprehensive testing program as part of ICT-risk management
Art 26/27
TLPT

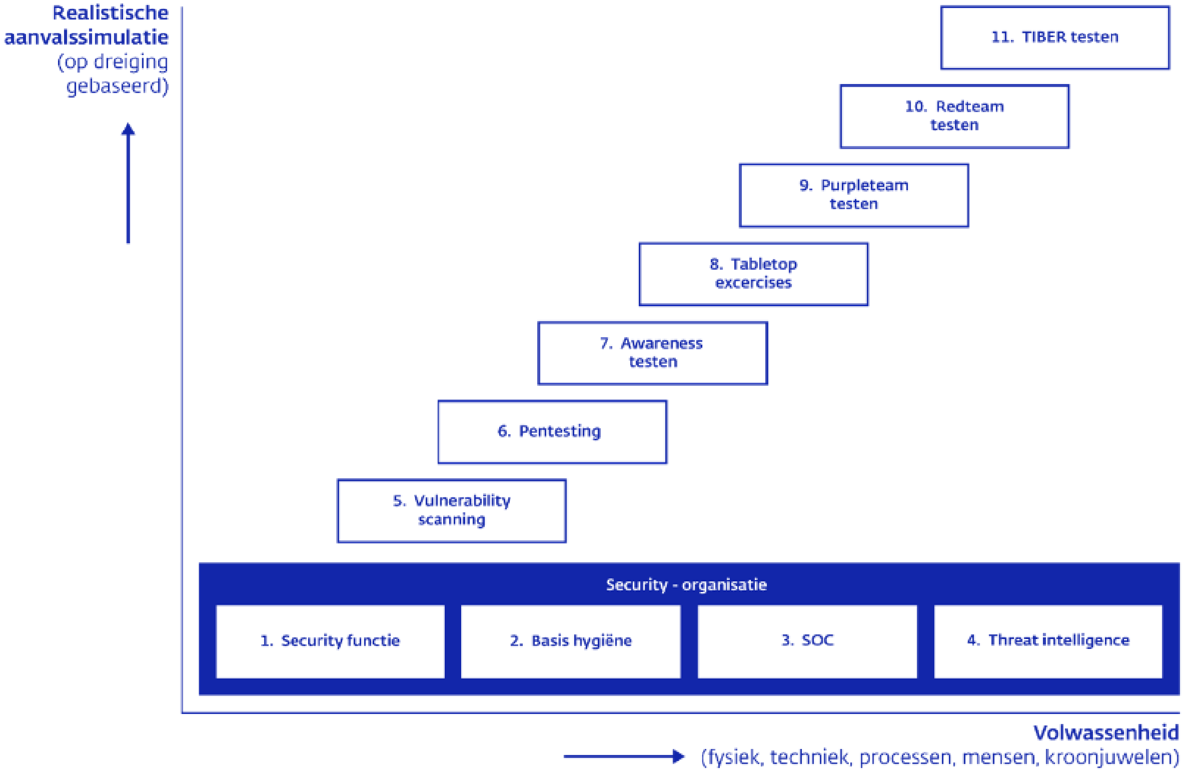
DeNederlandscheBank
EUROSYSTEEM

25(1) passende tests, zoals kwetsbaarheidsbeoordelingen en -scans, opensourceanalyses, netwerkbeveiligingsbeoor-delingen, kloofanalyses, beoordelingen van fysieke beveiliging, vragenlijsten en scanningsoftwareoplossingen, beoordelingen van broncodes indien mogelijk, scenariogebaseerde tests, compatibiliteitstests, prestatietests, eind-tot-eindtests en penetratietests.

25(1) appropriate tests, such as vulnerability assessments and scans, opensource analyses, network security assessments, gap analyses, physical security reviews, questionnaires and scanning software solutions, source code reviews where feasible, scenario-based tests, compatibility testing, performance testing, end-to-end testing and penetration testing.

DeNederlandscheBank
EUROSYSTEEM

Een model om tot een securitytest-roadmap te komen



Realistische aanvalssimulatie
(op dreiging gebaseerd)

11. TIBER testen
10. Redteam testen
9. Purpleteam testen
8. Tabletop excercises
7. Awareness testen
6. Pentesting
5. Vulnerability scanning

Security - organisatie

1. Security functie
2. Basis hygiëne
3. SOC
4. Threat intelligence

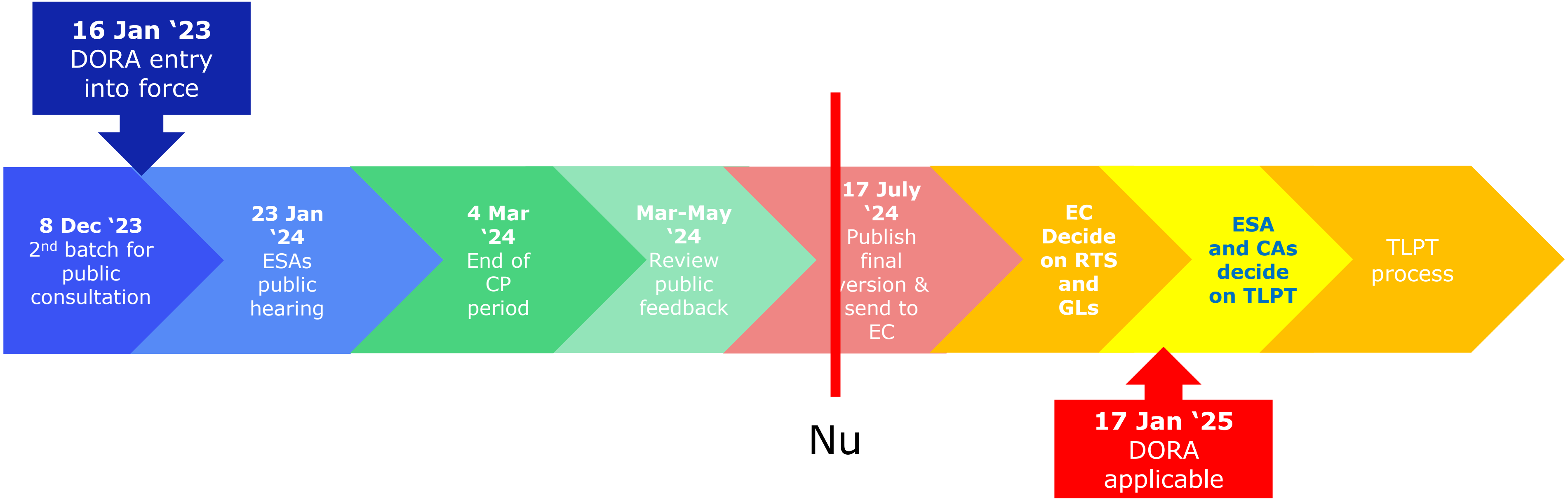
Volwassenheid
(fysiek, techniek, processen, mensen, kroonjuwelen)

Thread-Led Penetration Testing (TLPT)

- Financial institutions with major impact on financial stability
- TLPT versus TIBER
- Learning remains a focus
- *New:* roll of supervision
- *New:* pooled testing

DeNederlandscheBank
EUROSYSTEEM

Where are we now?



16 Jan '23
DORA entry into force

8 Dec '23
2nd batch for public consultation

23 Jan '24
ESAs public hearing

4 Mar '24
End of CP period

Mar-May '24
Review public feedback

17 July '24
Publish final version & send to EC

EC Decide on RTS and GLs

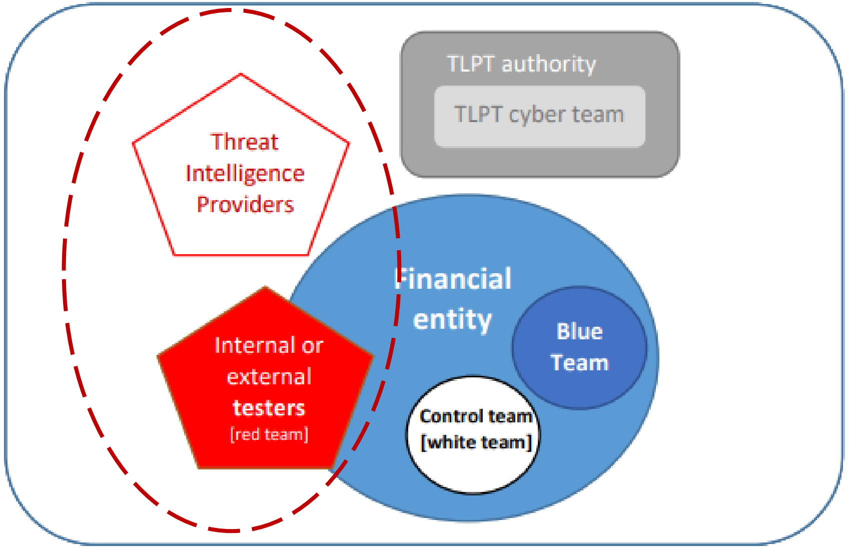
ESA and CAs decide on TLPT

TLPT process

Nu

17 Jan '25
DORA applicable

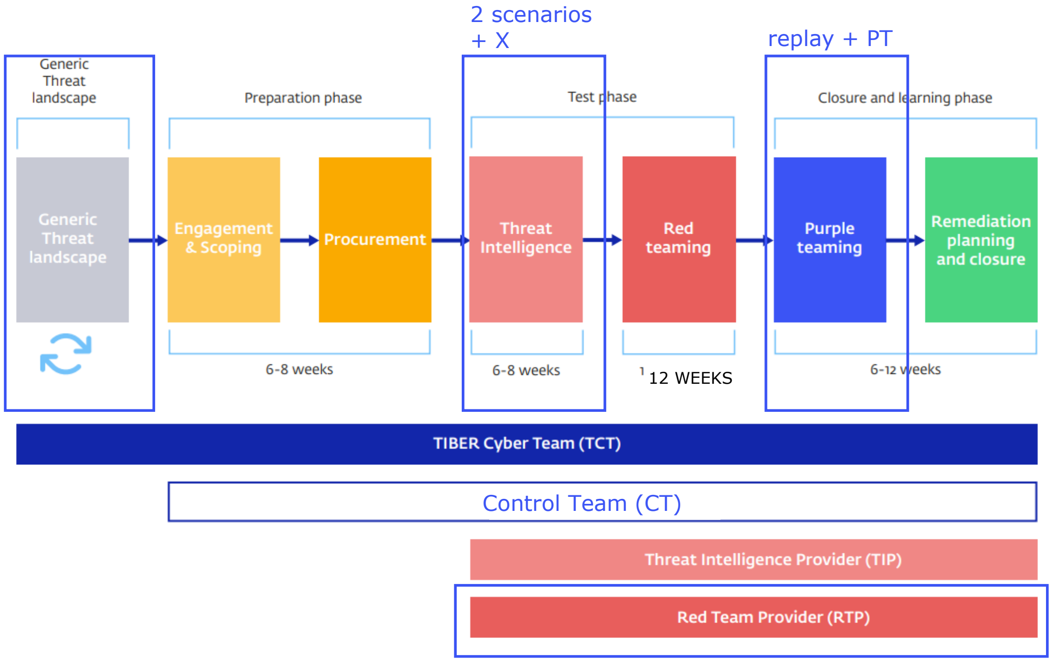
TLPT stakeholders


TLPT authority
TLPT cyber team
Threat Intelligence Providers
Financial entity
Blue Team
Internal or external testers [red team]
Control team [white team]

TLPT: process

- A risk assessment during the preparation phase is mandatory

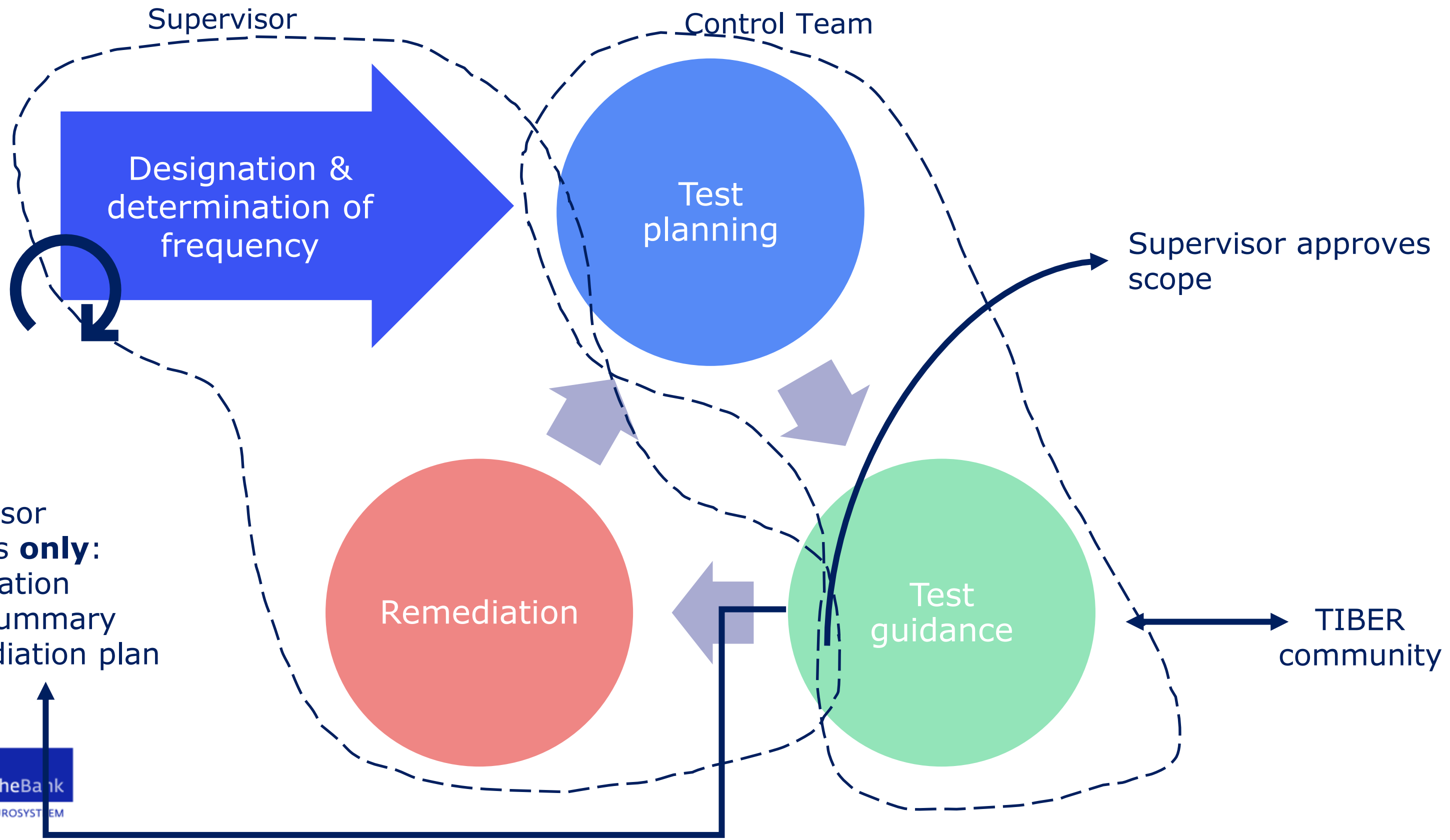
- Requirements for providers



not mandatory in TLPT

also internal testers

Role ECB / DNB Control Team vs. supervisor



Supervisor

Control Team

Designation & determination of frequency

Test planning

Supervisor approves scope

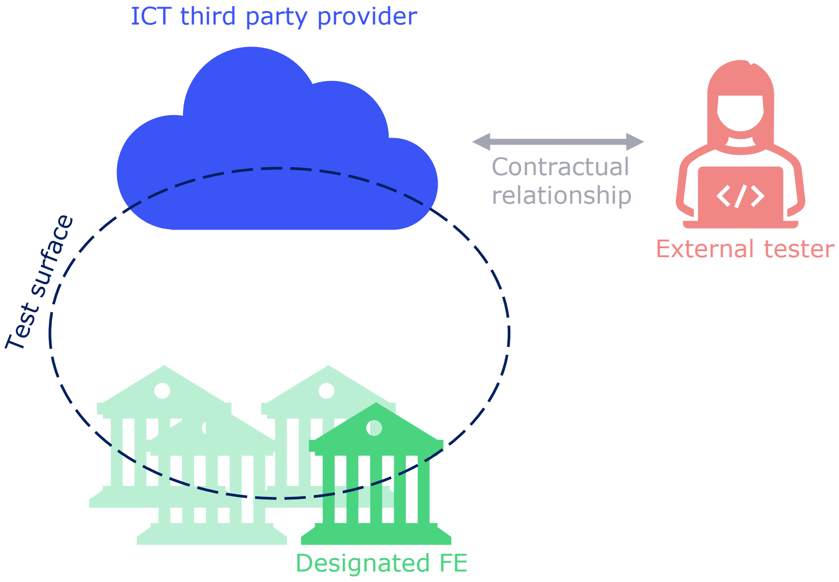
Remediation

Test guidance

TIBER community

Supervisor receives **only**:
- attestation
- test summary
- remediation plan

RTS: pooled testing



- Very few mentions of pooled testing
- f.e. no clear guidance on scoping in pooled test

Roll of IT auditors?

- 3rd LOD for the organisation
- Audit pro-active actions
  - Audit plan
  - Preparation for TLPT
- Audit re-active actions
  - Results of TLPT
  - Mitigation Plan
  - Monitoring

Crisis Management

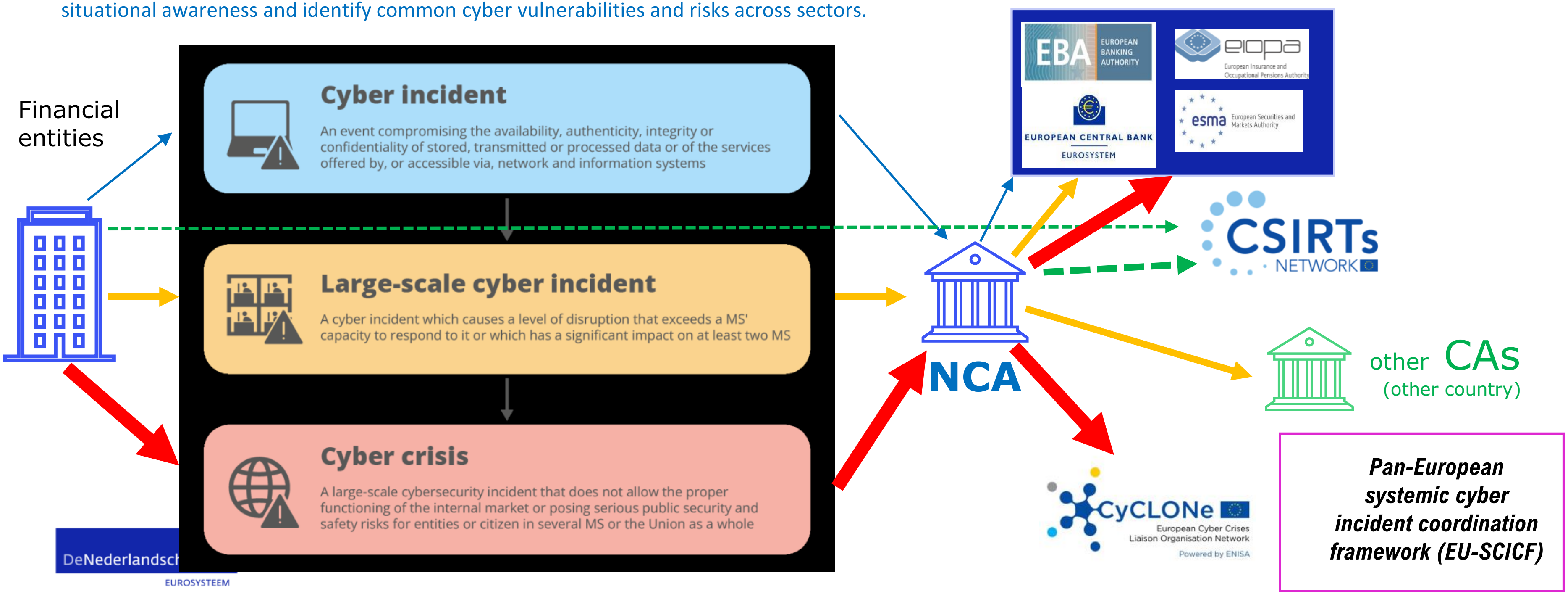
DeNederlandscheBank

EUROSYSTEEM

Crisis Management

Dora article 49: **Financial cross-sector exercises, communication and cooperation**

The ESAs, through the Joint Committee and in collaboration with competent authorities, resolution authorities, the ECB, the Single Resolution Board, the ESRB and ENISA, as appropriate, may establish mechanisms to enable the sharing of effective practices across financial sectors to enhance situational awareness and identify common cyber vulnerabilities and risks across sectors.



Cyber incident

An event compromising the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the services offered by, or accessible via, network and information systems

Large-scale cyber incident

A cyber incident which causes a level of disruption that exceeds a MS' capacity to respond to it or which has a significant impact on at least two MS

Cyber crisis

A large-scale cybersecurity incident that does not allow the proper functioning of the internal market or posing serious public security and safety risks for entities or citizen in several MS or the Union as a whole

Financial entities
NCA
EBA EUROPEAN BANKING AUTHORITY
eiopa European Insurance and Occupational Pensions Authority
EUROPEAN CENTRAL BANK EUROSYSTEM
esma European Securities and Markets Authority
CSIRTs NETWORK
other CAs (other country)
CyCLONe European Cyber Crises Liaison Organisation Network Powered by ENISA
Pan-European systemic cyber incident coordination framework (EU-SCICF)
DeNederlandsch EUROSYSTEEM

DORA

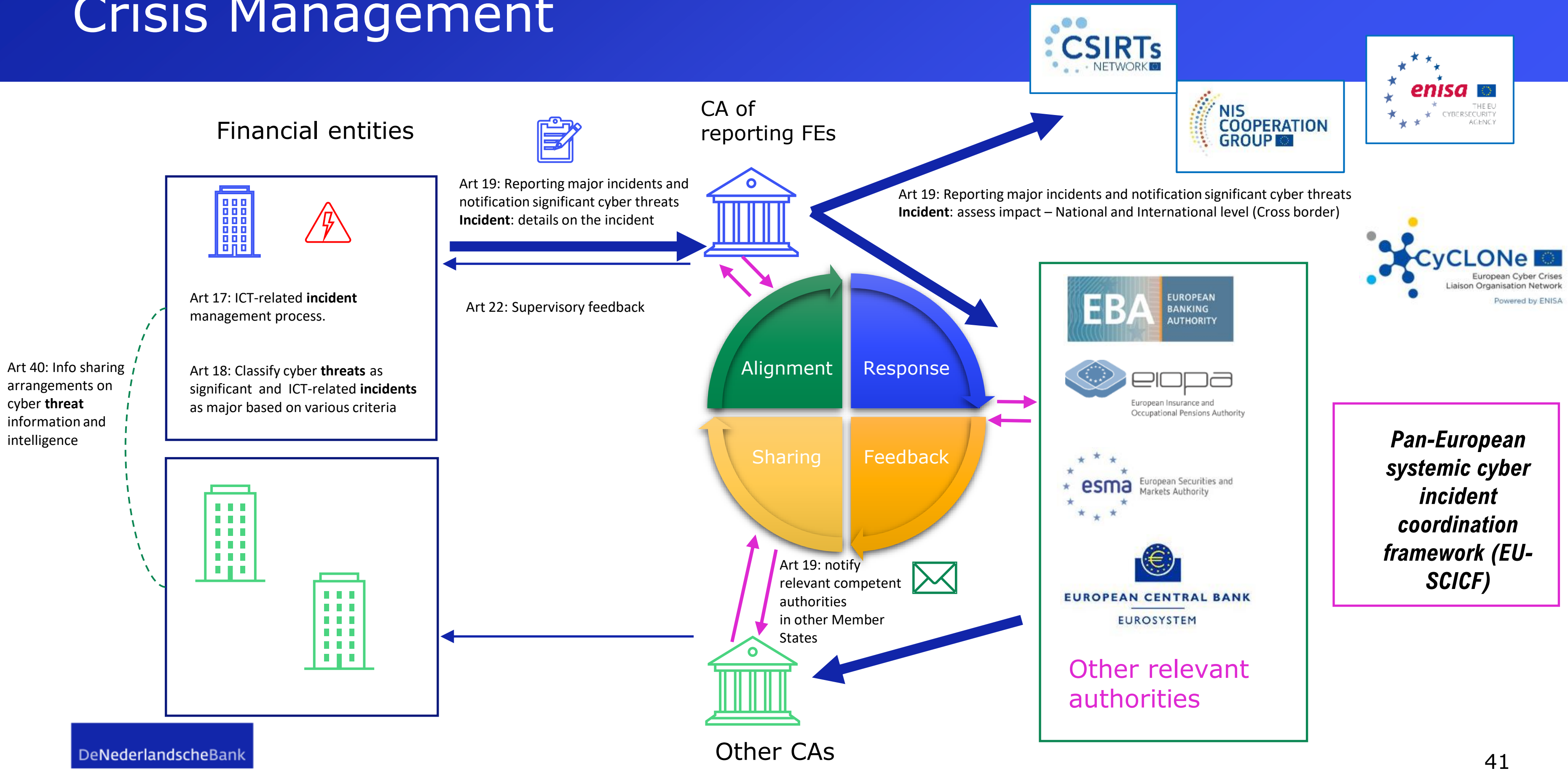
TLPT

Crisis Management

Resilience testing

m.h.e.m.van.beek@dnb.nl

Crisis Management



Financial entities

Art 17: ICT-related **incident** management process.

Art 18: Classify cyber **threats** as significant and ICT-related **incidents** as major based on various criteria

Art 40: Info sharing arrangements on cyber **threat** information and intelligence

Art 19: Reporting major incidents and notification significant cyber threats
Incident: details on the incident

Art 22: Supervisory feedback

CA of reporting FEs

Art 19: Reporting major incidents and notification significant cyber threats
Incident: assess impact – National and International level (Cross border)

Alignment

Response

Sharing

Feedback

Art 19: notify relevant competent authorities in other Member States

Other CAs

Other relevant authorities

Pan-European systemic cyber incident coordination framework (EU-SCICF)

CSIRTs NETWORK
NIS COOPERATION GROUP
enisa THE EU CYBERSECURITY AGENCY
CyCLONe European Cyber Crises Liaison Organisation Network
Powered by ENISA
EBA EUROPEAN BANKING AUTHORITY
eiopa European Insurance and Occupational Pensions Authority
esma European Securities and Markets Authority
EUROPEAN CENTRAL BANK
EUROSYSTEM