DORA

DORA – The next IT-regulation in the pipeline?

ISACA Squaretable

3rd May 2023

Contents

Introductions

Introduction Digital Operational Resilience Act (DORA)

DORA in Detail

What’s actually new? Comparison with existing frameworks

DORA Timeline to compliance

Urgency and challenges Asset management Sector

Who will be regulating DORA?

Consequences non-compliance

What needs to be done and can be done currently?

Q&A

Introduction

Ali Alam – KPMG Netherlands

- IT Advisor/Auditor
- KPMG DORA Working Group co-lead
- IT Risk in Control proposition lead.
- Extensive experience in conducting Maturity Assessments and implementations based on DNB Information Security Good Practice and EBA Guidelines at financial institutions

Introduction Digital Operational Resilience Act

What is DORA?

A “Regulation on **D**igital **O**perational **R**esilience **A**ct for the financial sector” (DORA).

DORA in force per 17th January 2023 and applicable for compliance per 17th January 2025.

DORA aims to implement a **uniform framework*** for the security of network and information systems used in the financial sector.

** To consolidate single ICT frameworks from the EBA, EIOPA, ESMA*

DORA will impact all financial entities regulated at the EU-level including:

- The Financial Services Industry
- Payment institutions
- **Investment firms/ managers of alternative investment funds**
- Credit rating agencies
- Crypto-asset service providers
- Crowdfunding service providers
- Fintech
- Trading venues
- Financial system providers
- Credit institutions
- ICT Service Providers (*in-scope providers to be designated by NCA**)

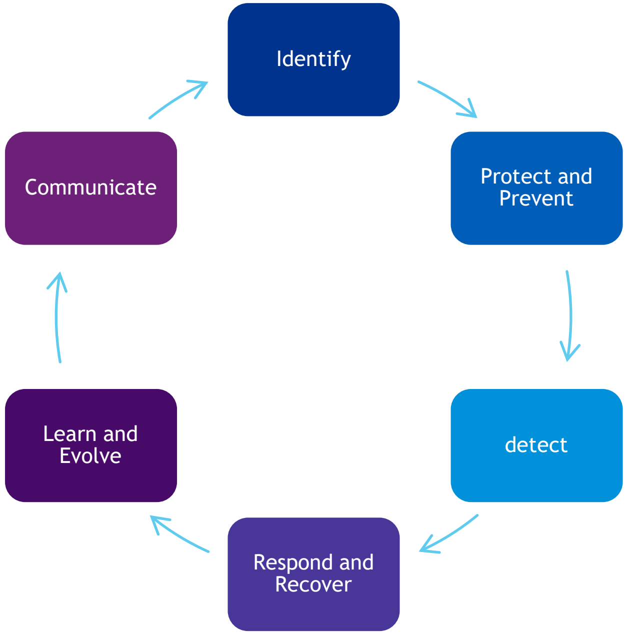
Chapter	II	III	IV	V	VI
	ICT risk management framework	Incident handling	Digital operational resilience testing	Managing of ICT third-party risks	Information sharing arrangements

** NCA: National Competent Authority*

How do financial institutions perceive DORA?

DORA in detail

ICT Risk Management



DORA requires from financial entities:

- Financial entities have an internal governance- and control framework
- Higher management carries end responsibility for ICT Risk Management within the entity
- Higher management puts in effort to keep knowledge and skills up to date in order to adequately address ICT risk
- Financial entities should have an ICT risk management framework which consists of strategies, policies, procedures and protocols to manage ICT risk in the widest sense of the word and all relevant ICT assets should be in scope.
- This ICT Risk management framework should be at least assessed on adequacy on a yearly basis and audited regularly by internal audit.
- ICT Risk Management also includes supporting processes such as continuity and crisis management and employee awareness.

Incident Reporting

General requirements

Reporting of major ICT-related incidents to competent authorities

Classification of major ICT-related incidents based on DORA criteria

Threat-Led Pentesting

Basic Testing

Threat-led Penetration Testing (TLPT)

DORA requirements:

- Financial entities should set up a broad operational resilience program.
- Security testing should be based on a thorough risk assessment and threat analyses of the financial entity so that testing is in line with threat landscape in which it operates
- Every three years, frequency may be adjusted
- Pen-testing (third) parties should be assessed on specific DORA requirements on knowledge, experience and skills

TIBER (Threat Intelligence-based Ethical Red-teaming)

Third party risk

General Principles

Harmonization of key elements of relationship with ICT third-party service providers

Union Oversight framework for critical ICT third-party service providers

DORA requires from financial entities:

- Financial entities should manage third party risk as an integral part of ICT risk
- Third parties should be administered in a "Register of Information" with thorough detail about the third party and whether these are critical or important third parties to the financial entity
- New third party agreements are reported to the regulator
- Specific requirements on circumstances that warrant contract termination
- Emphasis on monitoring and managing concentration risk
- For each phase in lifecycle (pre-contracting till termination) specific requirements are prescribed

Information sharing Arrangements

DORA requires from financial entities:

- Set up groups in which information for cyber threats is exchanged to together strengthen the sector as a whole
- Report to the regulator on participation and exiting such groups.

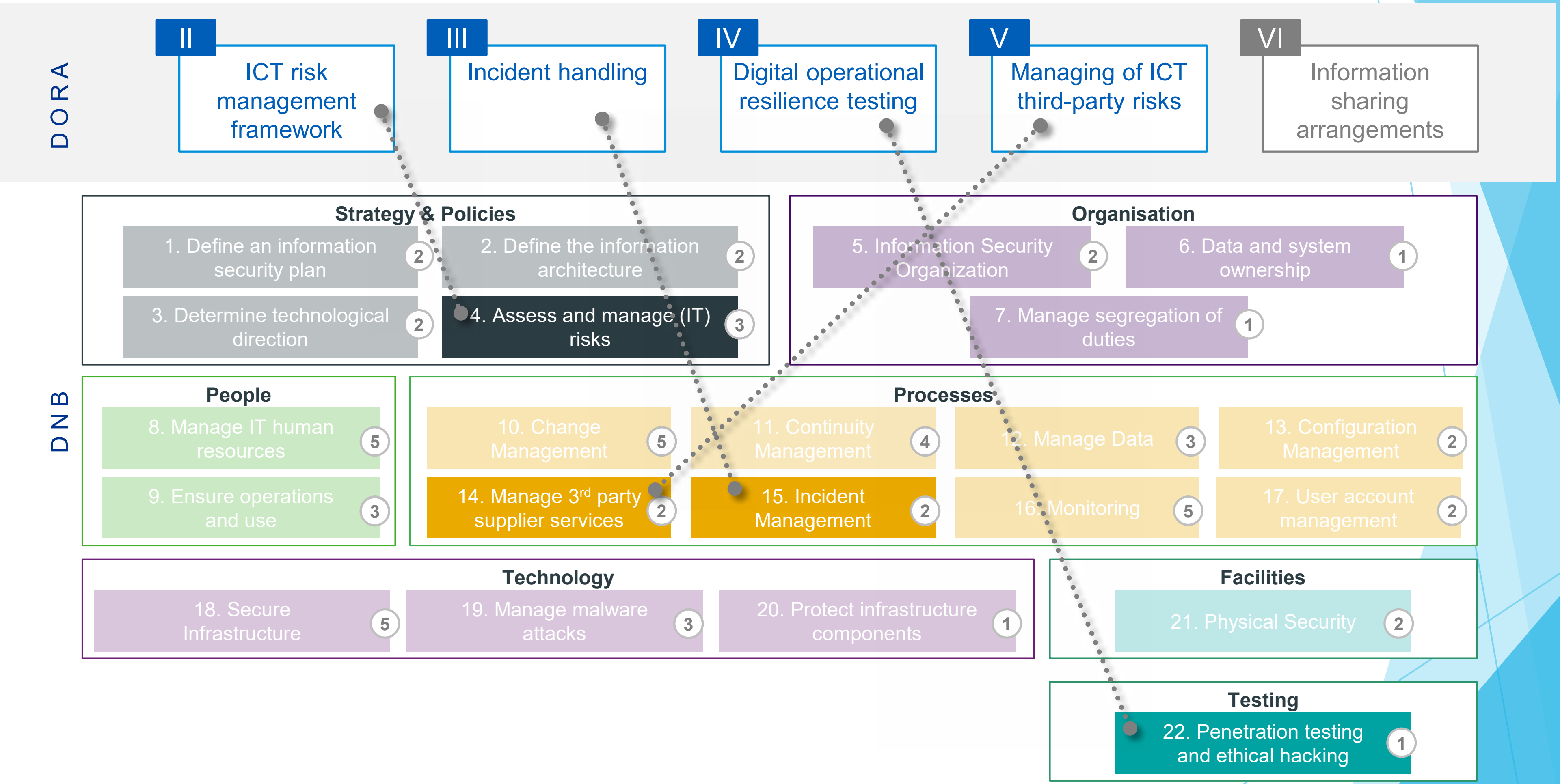
What’s actually new?

What is actually new?

- Within the asset management sector, there are three applicable frameworks:
  - DNB Good Practice Information Security 2019/2020
  - EBA Guidelines on ICT and security risk management (applies to investment firms only)
  - EBA Guidelines on outsourcing arrangements (applies to investment firms only)

- However DORA comes with requirements that are additional to the mentioned frameworks.

Overlap DNB IS Good Practice



DORA

II
ICT risk management framework

III
Incident handling

IV
Digital operational resilience testing

V
Managing of ICT third-party risks

VI
Information sharing arrangements

DNB

Strategy & Policies

1. Define an information security plan 2

2. Define the information architecture 2

3. Determine technological direction 2

4. Assess and manage (IT) risks 3

Organisation

5. Information Security Organization 2

6. Data and system ownership 1

7. Manage segregation of duties 1

People

8. Manage IT human resources 5

9. Ensure operations and use 3

Processes

10. Change Management 5

11. Continuity Management 4

12. Manage Data 3

13. Configuration Management 2

14. Manage 3rd party supplier services 2

15. Incident Management 2

16. Monitoring 5

17. User account management 2

Technology

18. Secure Infrastructure 5

19. Manage malware attacks 3

20. Protect infrastructure components 1

Facilities

21. Physical Security 2

Testing

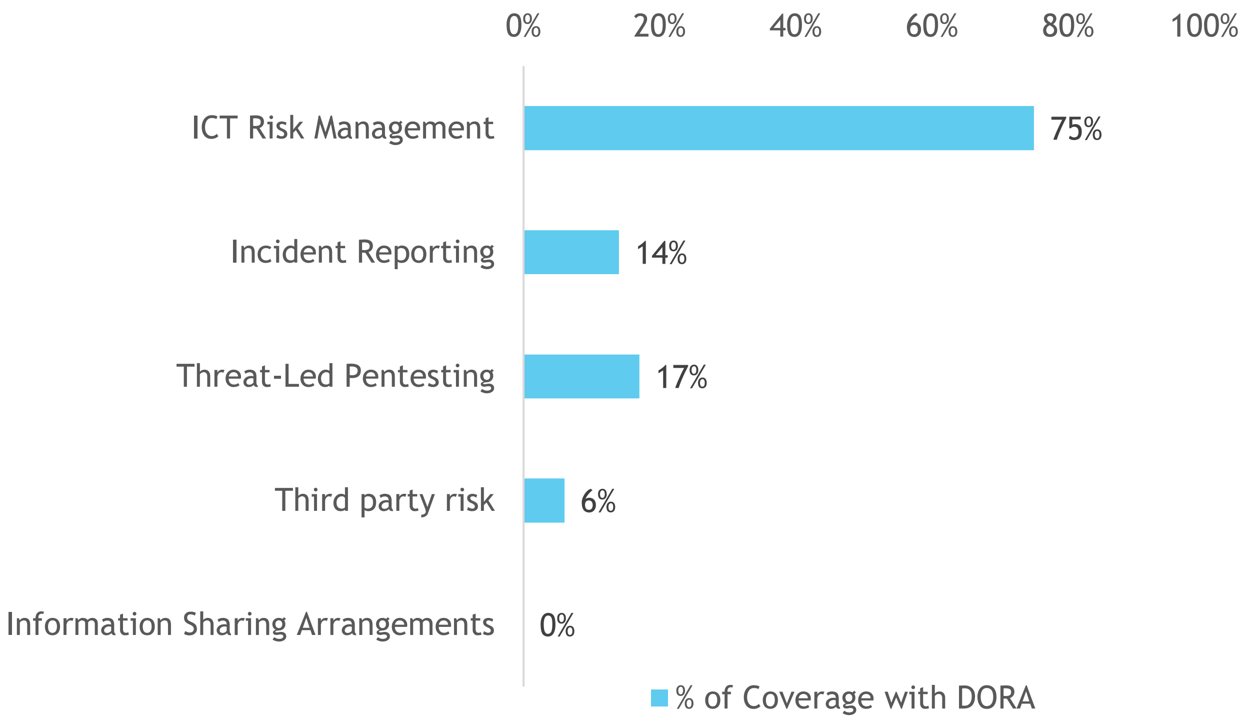
22. Penetration testing and ethical hacking 1

DORA deviates from the DNB IS Good Practice

DORA	In-depth controls More efforts to comply	Holistic approach Less effort to comply	DNB

II ICT risk management framework	III Incident handling	IV Digital operational resilience testing	V Managing of ICT third-party risks	VI Information sharing arrangements
– Specific requirements on the full ICT risk management cycle from identification to response and recovery, with additional emphasis on detection of risks and learning and evolving – ICT control testing needs to be done at least on an annual basis	– Reporting of major incidents to national competent authority (AFM) mandatory – Classification of incidents based on DORA requirements	– Additional requirement of threat-led penetration testing – Specific criteria apply to those who perform the different types of resilience testing	DORA requires third party risk management over the full lifecycle, being from pre-engagement due diligence till termination of contract and exiting strategies. DNB IS GP covers the performance management and risk assessments of existing contracts	Emphasis on exchange of cyber threat information and intelligence within trusted communities of financial entities, to the extent aimed at enhancing the digital operational resilience of all.
✓	✓	✓	✗	✓

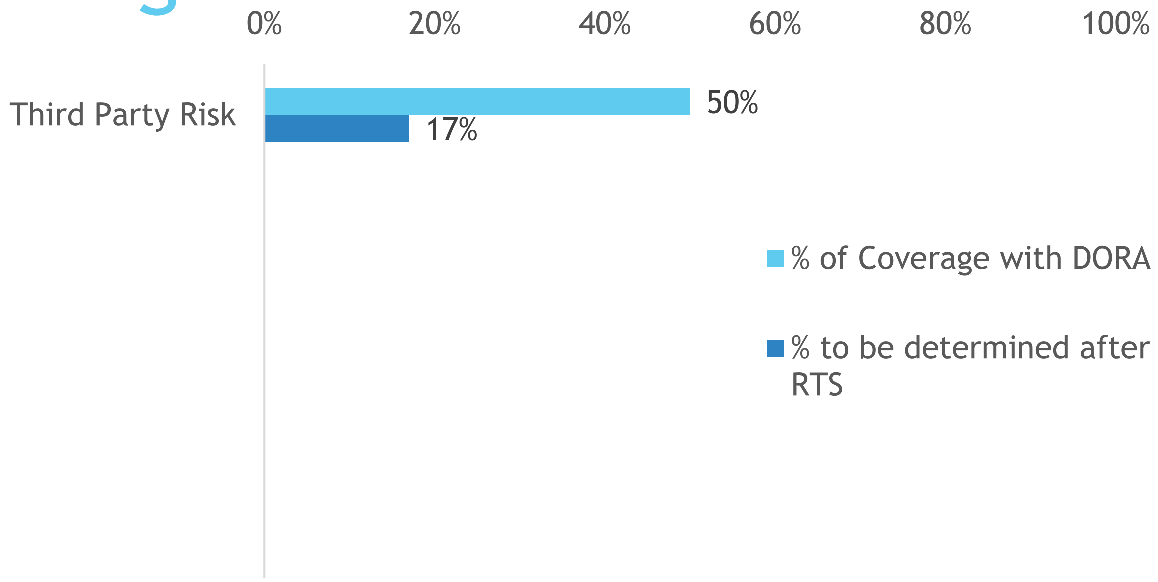
Overlap EBA Guidelines on ICT and security risk management



- Observations

- Risk management has the highest coverage, differences lie in:
  - DORA requiring management body of the financial entity to keep up to date with sufficient knowledge and skills to understand and assess ICT risk DORA taking into scope “all processes and ICT and information assets” as well as the ones delivered by ICT third party providers.
- Low coverage for Incident Reporting and Threat-Led Pentesting due to:
  - New DORA requirements on Incident classification and reporting requirements
  - New Threat-Led Pentesting requirements
- **Third Party Risk is addressed EBA Outsourcing Guidelines**
- **Information Sharing Arrangements has 0% coverage as its an entirely new topic.**
- **RTSs will provide further details.**

Overlap EBA Guidelines on outsourcing arrangements



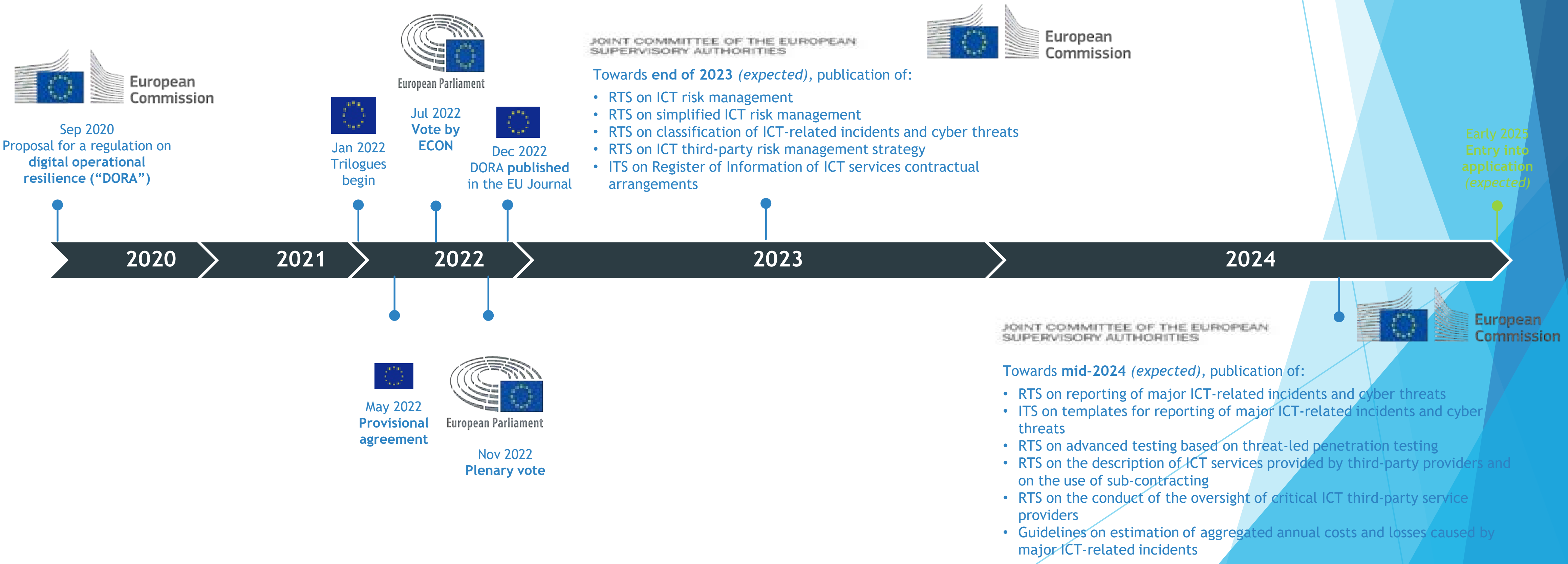
Observations

- **Difference lies in the level of detail of DORA vs EBA Outsourcing Guidelines**
- **A number of DORA articles are described on a higher level and will be further explained by the Regulatory technical standards later in 2023 and 2024.**

DORA Timeline to compliance

EU legislative process and timeline

- The finalization of DORA took place on track and publication in the EU official journal on 27th December 2022.
- This gives clients a two-year window to assess their compliance and plan the uplift of their internal arrangements by the entry into application of DORA which is expected no later than early 2025.
- In addition, the titles for the consultation papers for the first wave of RTS/ITS/GLs have been agreed.
- The first wave of consultation papers for the RTS/ITS/GLs are expected in May ‘23.



European Commission

Sep 2020
Proposal for a regulation on **digital operational resilience (“DORA”)**

Jan 2022
Trilogues begin

May 2022
Provisional agreement

European Parliament

Jul 2022
Vote by ECON

European Parliament

Nov 2022
Plenary vote

Dec 2022
DORA **published** in the EU Journal

JOINT COMMITTEE OF THE EUROPEAN SUPERVISORY AUTHORITIES

European Commission

Towards **end of 2023** *(expected)*, publication of:

- RTS on ICT risk management
- RTS on simplified ICT risk management
- RTS on classification of ICT-related incidents and cyber threats
- RTS on ICT third-party risk management strategy
- ITS on Register of Information of ICT services contractual arrangements

JOINT COMMITTEE OF THE EUROPEAN SUPERVISORY AUTHORITIES

European Commission

Towards **mid-2024** *(expected)*, publication of:

- RTS on reporting of major ICT-related incidents and cyber threats
- ITS on templates for reporting of major ICT-related incidents and cyber threats
- RTS on advanced testing based on threat-led penetration testing
- RTS on the description of ICT services provided by third-party providers and on the use of sub-contracting
- RTS on the conduct of the oversight of critical ICT third-party service providers
- Guidelines on estimation of aggregated annual costs and losses caused by major ICT-related incidents

Early 2025
Entry into application
(expected)

Urgency and challenges Financial Sector

- More mature financial institutions:

- Challenge to implement the multiple required regulations at the same time. Apart from DORA this includes EBA Guidelines on Outsourcing and Security, DNB Information Security Good Practice and the Corporate Sustainability Reporting Directive/ESG, EIOPA guidelines
- Challenges of complying with IT governance through compliance with the DNB Information Security Good Practice 2019/2020.

- This is caused by:

- Less regulatory activity from DNB on DNB Information Security Good Practice since 2010.
- Abundance of comparative frameworks that can give a headstart on building capabilities to comply with DORA.

- Less mature financial institutions

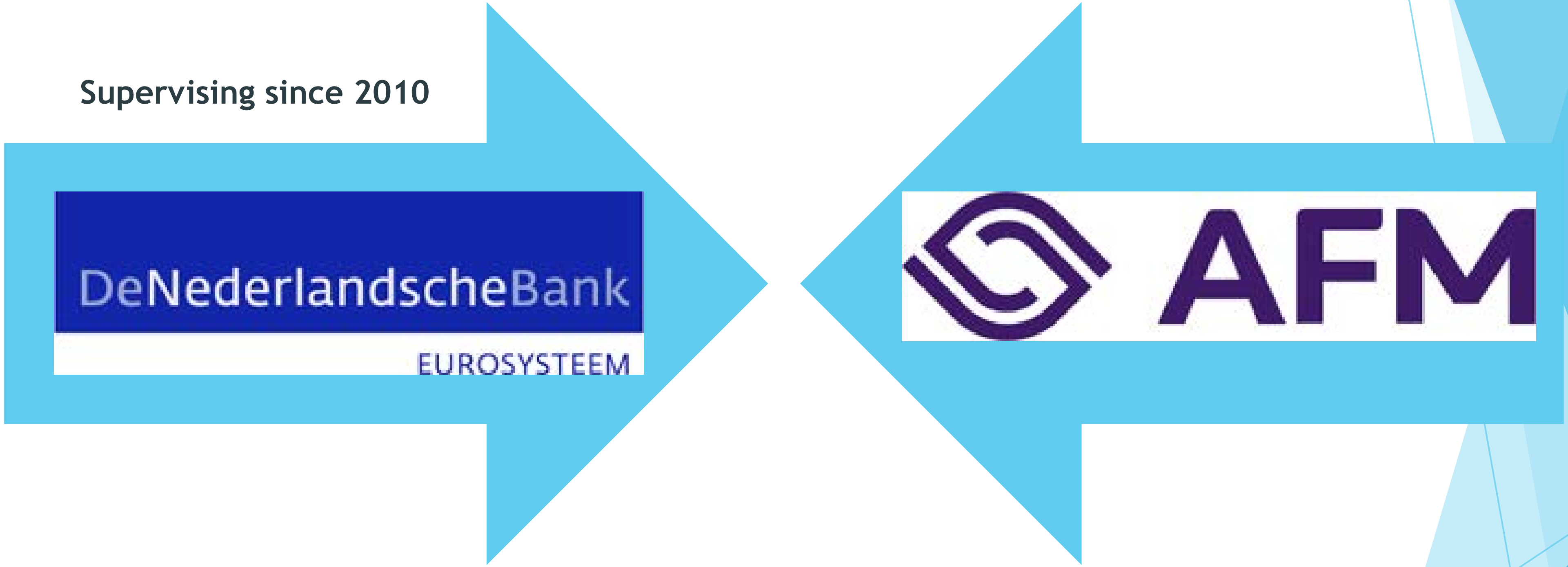
- No supported and demonstrated framework for IT and Information Cybersecurity
- Contracts with critical third party providers do not comply with DORA requirements
- Little experience with executing resilience testing
- Incident handling largely directed at business process incidents, rather than IT incidents

- This is caused by:

- Less regulatory activity from DNB on DNB Information Security Good Practice (asset management companies have mostly been regulated indirectly as service provider of other financial institutions, when required).
- Lack of comparative frameworks that can give a headstart on building capabilities to comply with DORA.

Who will be regulating DORA?

Supervising since 2010



Both are mentioning DORA in their recent publications!

Consequences non-compliance

- The regulation does not give any insight in how non-compliance with DORA is addressed by the NCA.
- However looking at existing conduct of the DNB we can infer and expect the following:

- The non-complying asset manager will come under tighter supervision by AFM/DNB, which includes delivery of an improvement plan and periodic reporting on progress to the AFM/DNB.
- Failure to improve could result into fines, warnings
- Ultimately resulting in revocation of the license to operate.

What needs to be done and can be done currently?

ICT Risk Management

- Evaluate whether the current ICT risk management process and control framework sufficiently covers the detailed requirements of DORA.

Incident Reporting

- Evaluate whether the current incident management process can be adapted to comply with the additional DORA classification requirements as well as setting up the reporting lines to the NCA on Major ICT incidents

Threat-Led Pentesting

- Evaluate and where needed revise strategy for penetration testing as DORA requires a more detailed threat analysis to determine the required penetration testing

Third party risk

- **Evaluate the criticality of your ICT thirdparties.**
- Create a Register of Information on ICT third party providers.
- Review existing third party contracts against DORA requirements.

Information sharing Arrangements

- Form a information sharing groups among your segment peers and discuss cybersecurity en information security risks

Q&A

WOENSDAG 10 MEI 2023
17:30 – 21:30 uur

ISACA®
Netherlands Chapter

ROUND TABLE

YOUR SPEAKER

WINN SCHWARTAU