

Nordic Region

Experiences with DORA Implementations in the Nordic Region

PECB REGIONAL WEBINARS



Jakob Seierø

Founder of Cyber Security Innovation ApS,
CyberSundhed and CyberEd
Denmark

Agenda

1. What is DORA and Why do we need it?
2. Compliance V.S. Maturity
3. How to eat an elephant called DORA?
4. “It all depends”
5. Key takeaways

What is DORA and why do we need it?

DORA

- The **Digital Operational Resilience Act** (DORA) is an EU regulation that entered into force on 16 January 2023 and will apply as of 17 January 2025.
- It aims at strengthening the IT security of financial entities such as banks, insurance companies and investment firms and making sure that the financial sector in Europe is able to stay resilient in the event of a severe operational disruption.
- Regulation - 2022/2554 - EN - DORA - EUR-Lex (europa.eu)

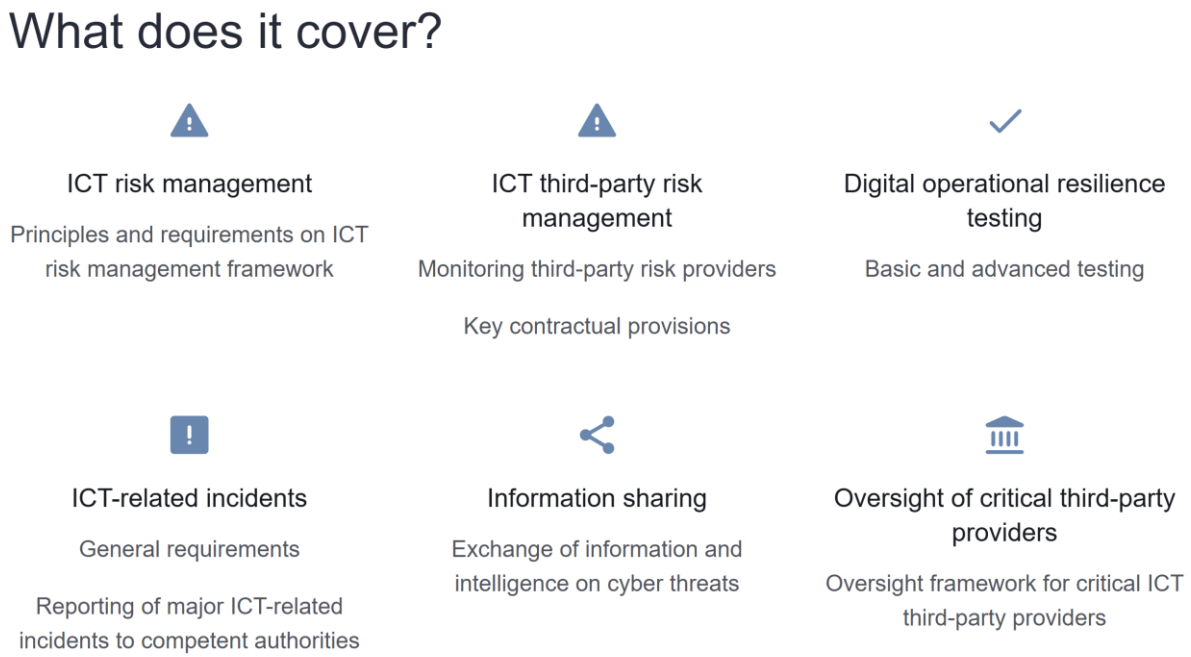
What does it cover?

Digital Operational Resilience Act (DORA) - European Union (europa.eu)

- CHAPTER I, General provisions, Article 1-4
- CHAPTER II, ICT risk management, Section I, Article 5-16
- CHAPTER III, ICT-related incident management, classification and reporting, Article 17-23
- CHAPTER IV, Digital operational resilience testing, Article 24-27
- CHAPTER V, Managing of ICT third-party risk, Section I, Key principles for a sound management of ICT third-party risk, Article 28-44
- CHAPTER VI, Information-sharing arrangements, Article 45
- CHAPTER VII, Competent authorities, Article 46-56
- CHAPTER VIII, Delegated acts, Article 57

What does it cover?

[Digital Operational Resilience Act (DORA) - European Union (europa.eu)]



Compliance V.S. Maturity

Compliance

- Either you are Compliant or not
- Documentation and evidence is key
- Shared and delegated decision making
- Non-compliant, then what

Maturity

- Gap-analysis as a starting point
- CMMC as a measurement for improvement
- Operational challenge

Compliance V.S. Maturity

- Compliance do not care about maturity
- Documentation and evidence are more important than operational challenges

- Deadline is 17th January 2025
- Focus on Compliance before the 17th January 2025 and Maturity after the 17th of January 2025

How to eat an elephant called DORA

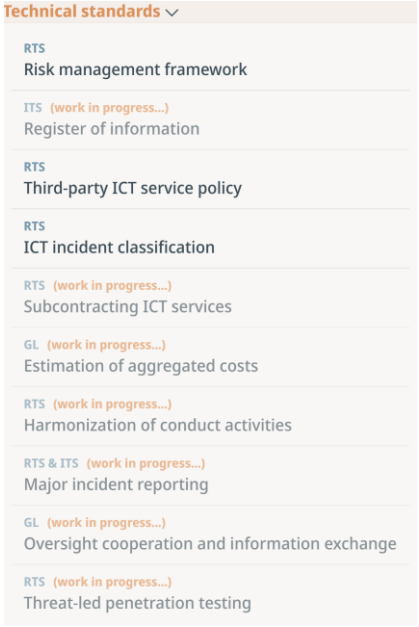
The elephant has 45 articles…

Digital Operational Resilience Act (DORA) - European Union (europa.eu)

- CHAPTER I, General provisions, Article 1-4
- CHAPTER II, ICT risk management, Section I, Article 5-16
- CHAPTER III, ICT-related incident management, classification and reporting, Article 17-23
- CHAPTER IV, Digital operational resilience testing, Article 24-27
- CHAPTER V, Managing of ICT third-party risk, Section I, Key principles for a sound management of ICT third-party risk, Article 28-44
- CHAPTER VI, Information-sharing arrangements, Article 45
- CHAPTER VII, Competent authorities, Article 46-56
- CHAPTER VIII, Delegated acts, Article 57

And the delegated elephants are partly here

[DORA (Digital operational resilience act) - Full legal text (dora-info.eu)]



CHAPTER VIII

Delegated acts

Article 57

Exercise of the delegation

1. The power to adopt delegated acts is conferred on the Commission subject to the conditions laid down in this Article.

2. The power to adopt delegated acts referred to in Articles 31(6) and 43(2) shall be conferred on the Commission for a period of five years from 17 January 2024. The Commission shall draw up a report in respect of the delegation of power not later than nine months before the end of the five-year period. The delegation of power shall be tacitly extended for periods of an identical duration, unless the European Parliament or the Council opposes such extension not later than three months before the end of each period.

Start form the top

- CHAPTER I, General provisions, Article 1-4 (Read and understand)
- CHAPTER II, ICT risk management, Section I, Article 5-16 (Step 1 is Governance and Risk)
- CHAPTER III, ICT-related incident management, classification and reporting, Article 17-23 (Step 2)
- CHAPTER IV, Digital operational resilience testing, Article 24-27 (Step 3 or 2)
- CHAPTER V, Managing of ICT third-party risk, Section I, Key principles for a sound management of ICT
- Third-party risk, Article 28-44 (Step 4 or 2)
- CHAPTER VI, Information-sharing arrangements, Article 45 (Step 5 or 2)
- CHAPTER VII, Competent authorities, Article 46-56(Read and understand)
- CHAPTER VIII, Delegated acts, Article 57(Read and evaluate which ones you shall implement)

Finish one article

How to Finish and be ready for audit

(Prerequisite is that a Gap-analisys has been done)

1. Prepare the project participants
2. Perform Workshops
3. Document decissions
4. Review and update governance documents(Policies, Guidelines and SOPs)
5. Review supporting systems and tooling
6. Test the new governance documents and supporting systems
7. Document and gather evidence
8. Hand-over to operations

It all depends…

On who you are

1. CISO
2. CTO
3. CRO
4. Procurement manager
5. Attorney
6. Board member
7. Compliance officer
8. HR Manager

What should we do?

Enterprise Risk Management	CTO	CISO
• ?	• ?	• ?
• **?**	• **?**	• **?**

Legal	Procurement	Compliance
• ?	• ?	• ?
• **?**	• **?**	• **?**

HR	Board of Directors	Who did we forget?
• ?	• ?	• ?
• **?**	• **?**	• **?**

Key takeaways

If you only do one thing do this

Read the Articles from the top
&
Know your accountability/responsibility

Secondly and Thirdly

Prioritize your articles from the top

Implement one article fully

Everything else you will learn by doing…

Document you decissions

Gather evidence

Have fun…
You are making the world a better place ☺

Q&A Session



Contact

- Website: www.cybersecurityinnovation.dk
- Phone: +45 26147007
- Email: jakob@cybersecurityinnavation.dk

For any questions or comments you can contact us below:

- support@pecb.com