How to ensure security following DORA regulation with less stress

Tomas Stamulis, Information Security Team Manager

June 13th, 2024

Digital Operational Resilience Act

- Designed to improve the cybersecurity and operational resiliency
- Defines requirements concerning the security of network and information systems supporting the business processes

What to do?

Stop wasting Your time

DORA will apply from 17 January 2025

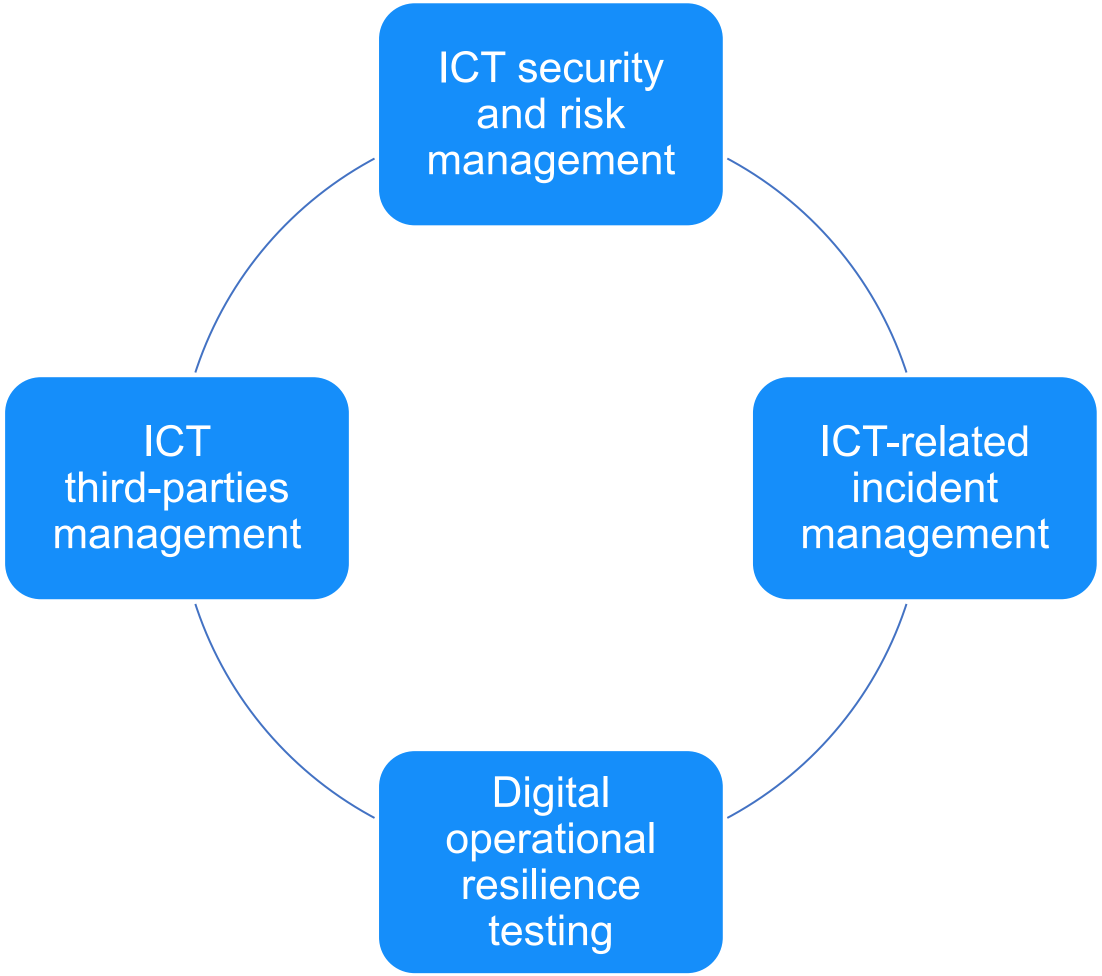
baltic amadeus

What to do?

1. Perform Gap analysis (internal or external assessment)
2. Prepare roadmap
3. Define roles and responsibilities
4. Implement identified gaps

How?

- Train
- Identify
- Define
- Establish
- Approve
- Implement
- Test
- Improve



ICT security and risk management

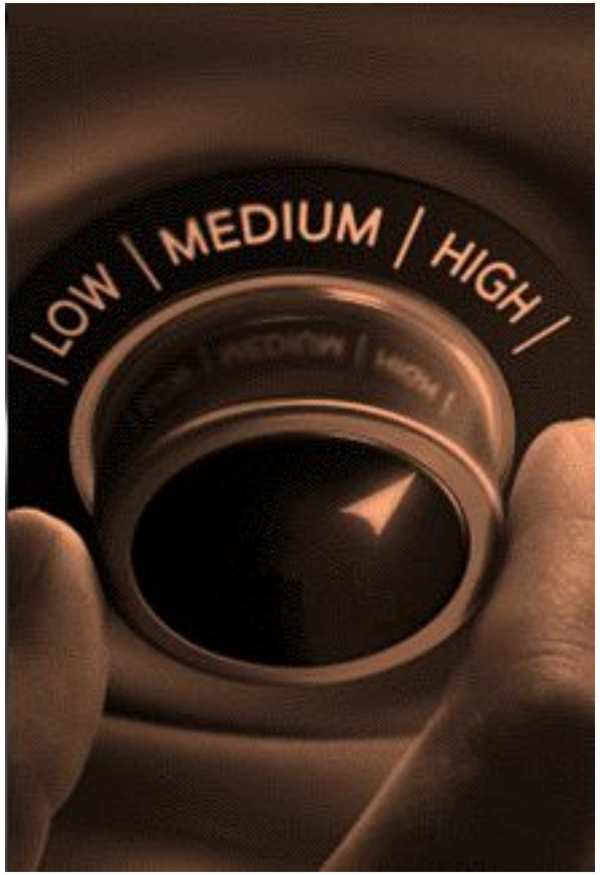
ICT-related incident management

Digital operational resilience testing

ICT third-parties management

Identification

1. Identify critical business activities and supporting business activities
2. Set out criticality of business activities
3. Map business activities with Information assets and ICT assets
4. Create Information asset inventory register
5. Create ICT register and map with Information assets
6. Identify ICT third parties and dependences from them



Define, Establish and Approve

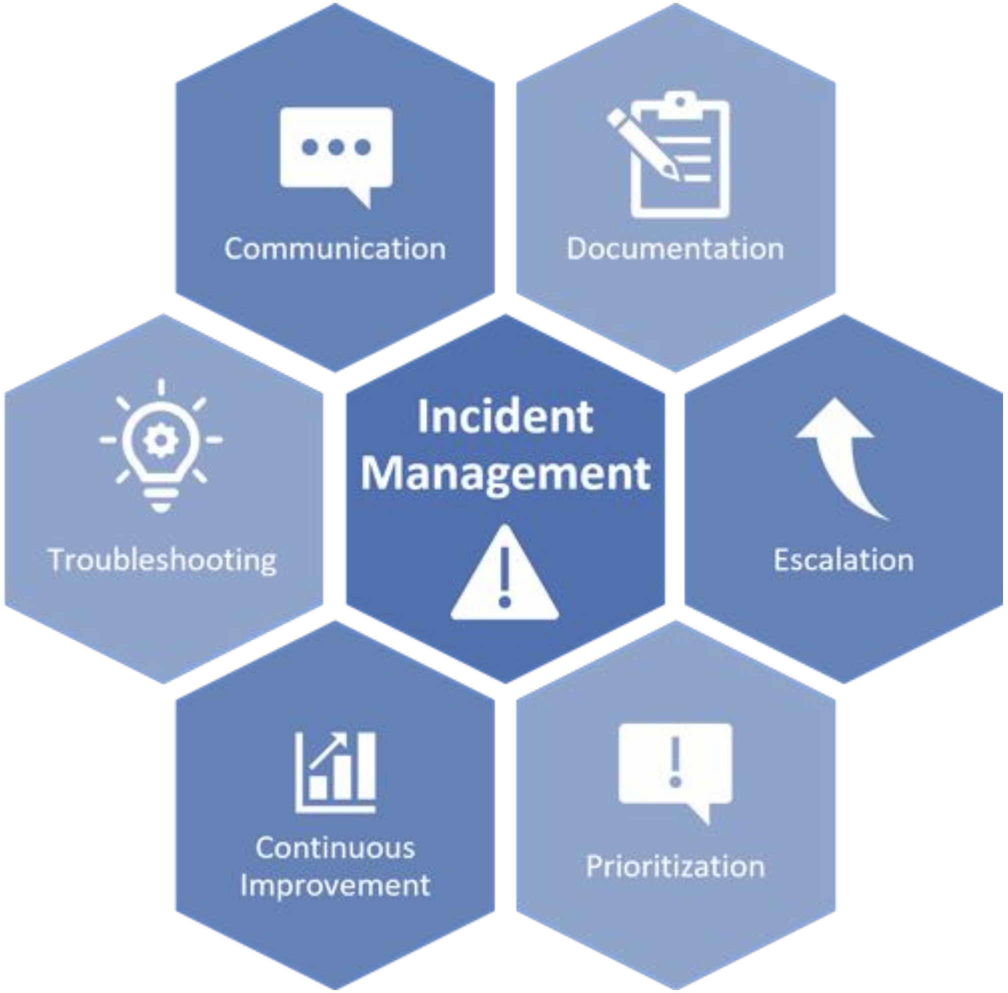
ICT risk framework including:

- **Information security policy (policies)**
- **Risk management policy and procedure**
- **Business continuity plan**
- **Backup and restoration procedure**
- **ICT operations management procedure**
- **Information classification and management procedure**
- **Access Management and Control procedure**
- **Logging and Monitoring procedure**
- **ICT Change Management procedure**
- **…**

Define, Establish and Approve

ICT-related incident management procedure including:

- Roles and responsibilities
- Detection on incidents and anomalies
- Reporting to responsible personnel
- Evaluation of information
- Classification and prioritization
- Analysis
- Management of incident
- Reporting to stakeholders and supervisory authorities
- Internal and external communication
- Lessons learned



Define, Establish and Approve

Digital operational resilience testing program including:

- ▯ Vulnerability assessment and scans
- ▯ Internal and external network security assessment
- ▯ Security compliance assessment
- ▯ Security architecture assessment
- ▯ Physical security assessment
- ▯ Performance testing
- ▯ Penetration testing
- ▯ Source code review
- ▯ Red teaming exercise
- ▯ Advances testing based on TLPT (if necessary)

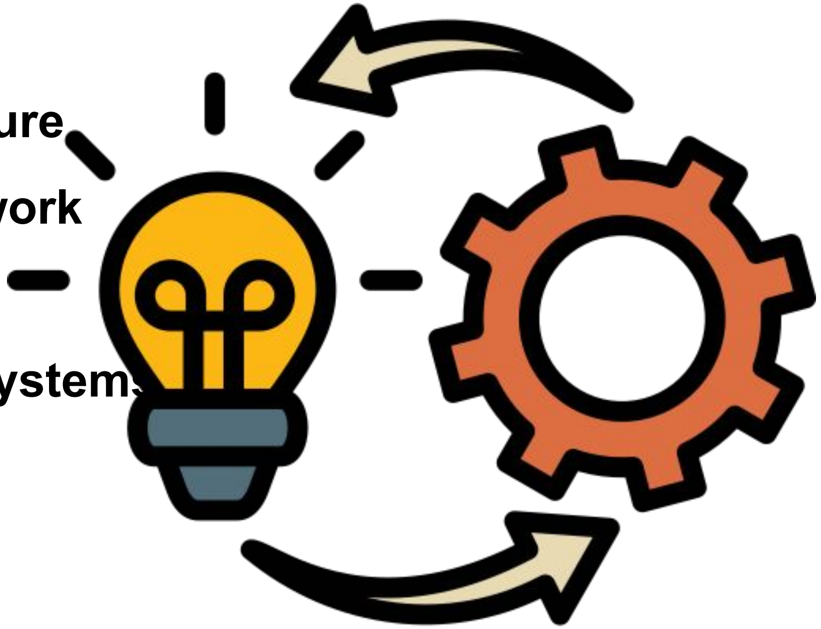
Define, Establish and Approve

ICT third party management including:

- **ICT third party management policy**
- **ICT security and other requirement for ICT third party**
- **Requirement for contractual arrangements**
- **ICT third party management procedure**
- **Initial and regular evaluation of ICT third parties**
- **Exit strategies**

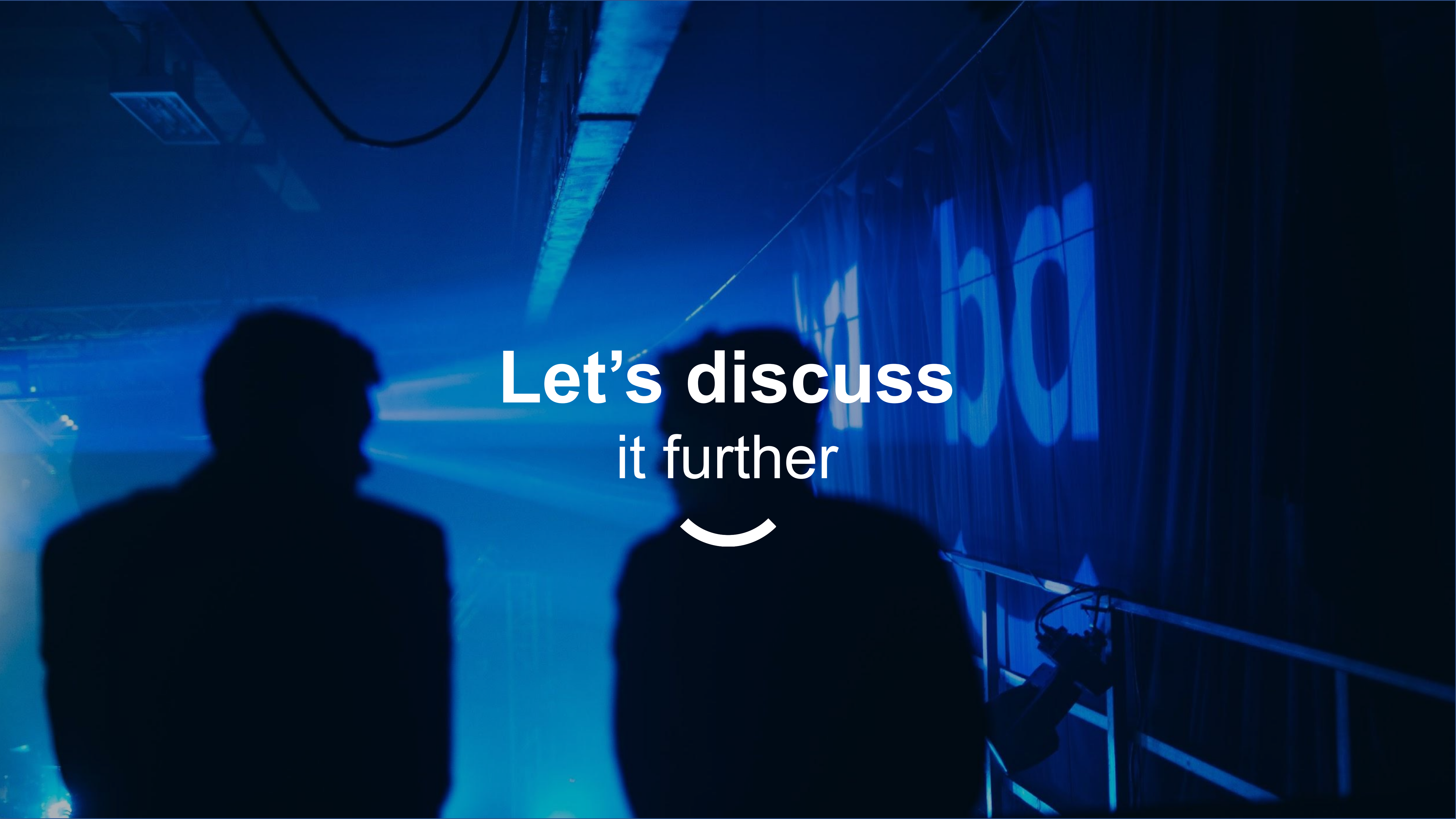
Implement

- Assign roles
- Introduce responsibilities
- Evaluate current ICT systems, infrastructure and security architecture
- Adopt current systems, application, tools following ICT risk framework requirement
- Identify and implement necessary additional ICT tools, solutions, systems
- Identify and implement additional security tools and solutions
- Train staff



Takeaways

- DORA compliance implementation is not one person or team show
- Split activities and responsibilities
- Management support is crucial
- Only 7 months left till deadline
- Digital operational resilience is continuous activity



Let’s discuss

it further

baltic amadeus

Let's discuss it further

TOMAS STAMULIS

INFORMATION SECURITY TEAM MANAGER

☎ +370 652 73676

✉ t.stamulis@ba.lt

in Tomas Stamulis