# Digital operational resilience act (DORA)

Slaven Smojver, PhD, CRISC, CISM, CISA
slaven.smojver@gmail.com

December, 2022

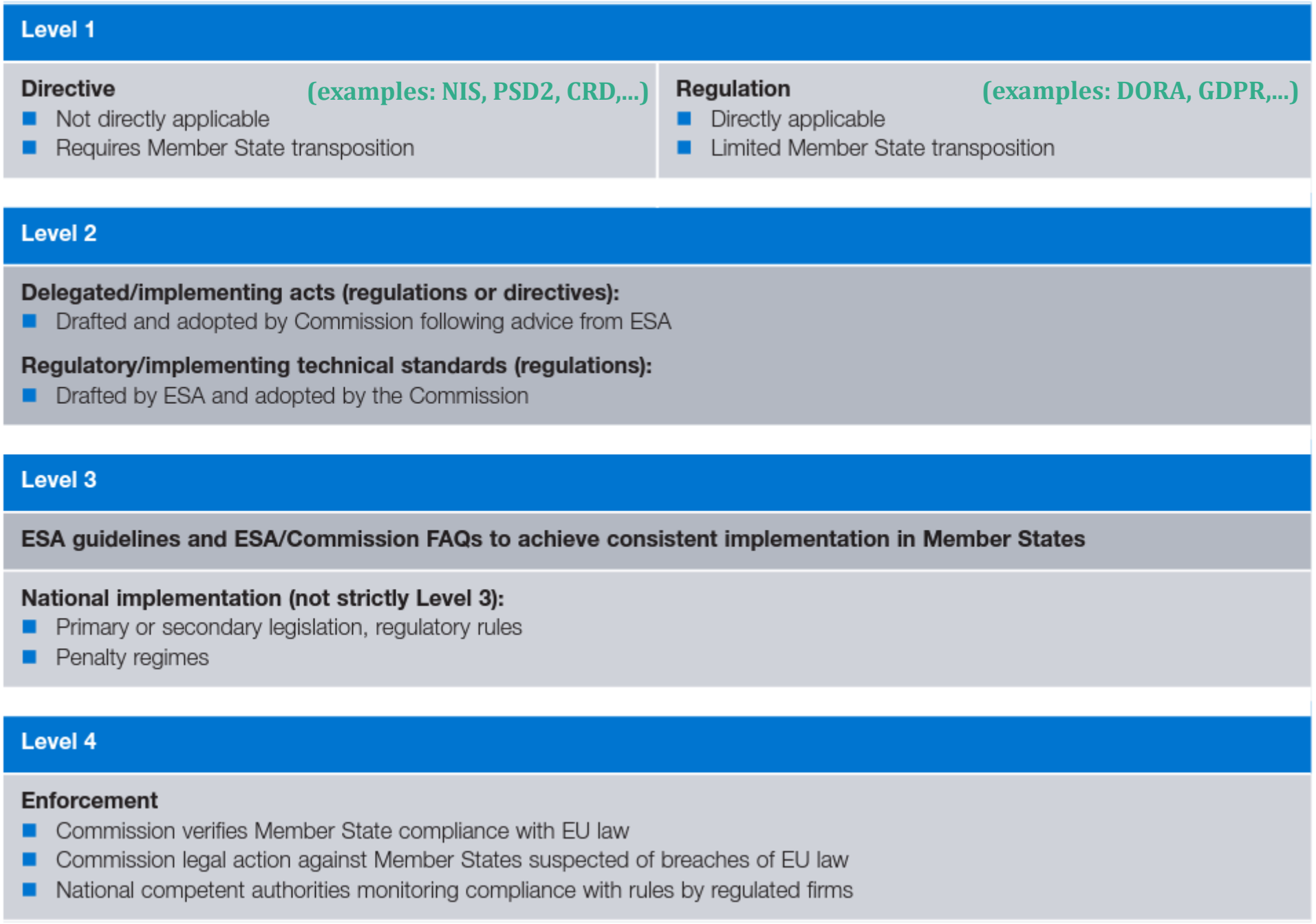
**The views expressed in this presentation do not necessarily reflect the views of the Croatian National Bank**

Photo by Jonathan Taylor on Unsplash

# Types of EU legislation

| | |
|---|---|
| **Regulations** | A binding legislative act. It must be applied in its entirety across the EU. (examples: DORA, GDPR,...) |
| **Directives** | A legislative act that sets out a goal that all EU countries must achieve. However, it is up to the individual countries to devise their own laws on how to reach these goals. (examples: NIS, PSD2, CRD,...) |
| Decisions | A "decision" is binding on those to whom it is addressed (e.g. an EU country or an individual company) and is directly applicable. |
| Recommendations | A "recommendation" is not binding. A recommendation allows the institutions to make their views known and to suggest a line of action without imposing any legal obligation on those to whom it is addressed. |
| Opinions | An "opinion" is an instrument that allows the institutions to make a statement in a non-binding fashion, in other words without imposing any legal obligation on those to whom it is addressed. An opinion is not binding. |

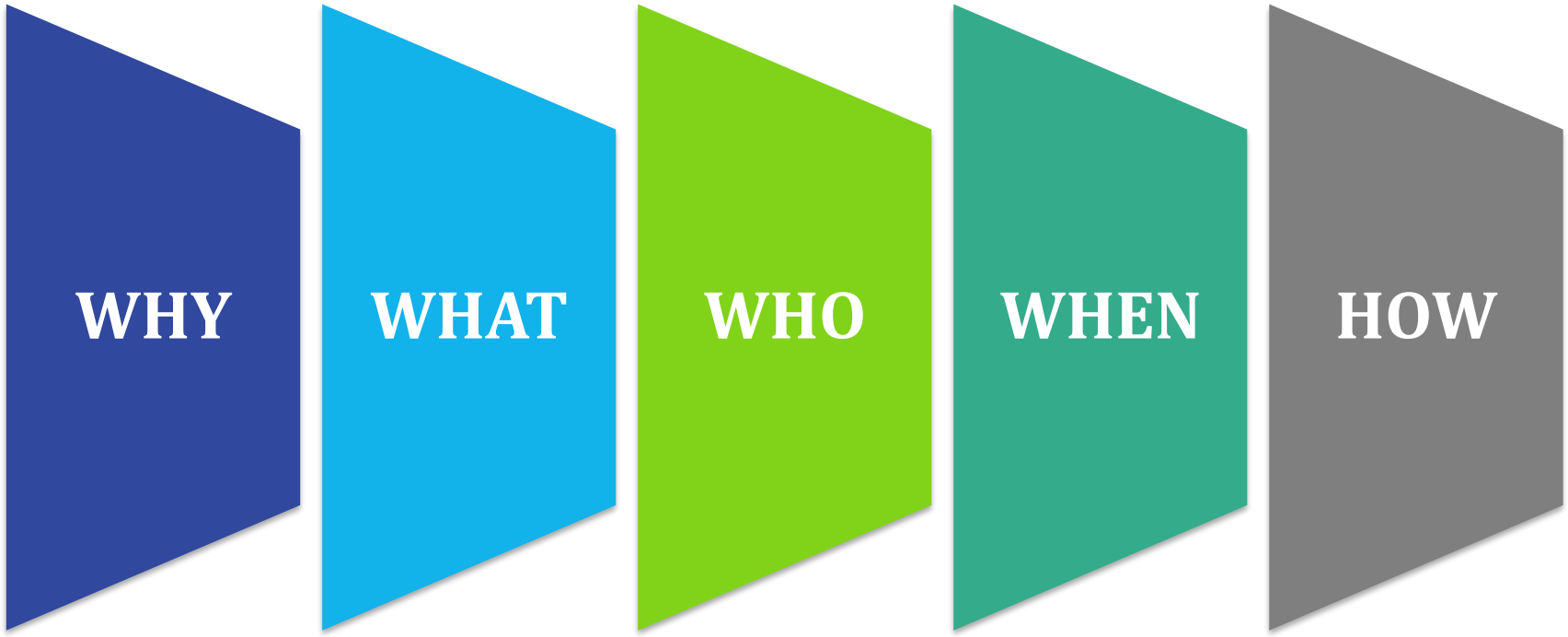
Source: https://european-union.europa.eu/institutions-law-budget/law/types-legislation_en




In the financial services sector, Level 1 Directives and Regulations rarely provide the complete picture that firms need in order to comply with new rules. "Level 2" measures are frequently used to provide the requisite detail in the form of either delegated acts or implementing acts (which may take the form of regulatory or technical implementing standards prepared by one or more of the ESAs).

Source: https://www.cliffordchance.com/content/dam/cliffordchance/briefings/2016/09/the-eu-legislative-process-explained.pdf

# Digital Operational Resilience Act (DORA)



# The EU Digital Finance Package (2020)

**WHY**

- The **digital finance strategy** (DFS) sets out general lines on how Europe can support the digital transformation of finance in the coming years, while regulating its risks.
- The strategy sets out four main priorities:
  - removing fragmentation in the Digital Single Market,
  - adapting the EU regulatory framework to facilitate digital innovation,
  - promoting a data-driven finance and
  - addressing the challenges and risks with digital transformation, including enhancing the **digital operational resilience of the financial system.**

# Digital Operational Resilience Act (DORA)

**WHAT**

- DORA outlines uniform requirements for the **security of network and information systems** of companies and organizations operating in the **financial sector** as well as critical third parties which provide ICT related services such as cloud platforms or data analytics services.
- DORA forms parts of a larger digital financial package which aims at developing a European approach fostering technological development and ensuring financial stability and consumer protection.
- DORA vs NIS2 vs. CER
  - DORA is *lex specialis* for Financial Entities (FE) in respect to NIS2 (new directive on security of network and information system), which replaces the current directive on security of network and information systems (NIS).
  - Critical Entity Resilience Directive (CER) complements NIS2 to form a common framework to protect 'key operators' active in the EU.

WHAT

# The Main Areas of DORA

**ICT Risk Management**

**ICT Incident Reporting**

**Digital Operational Resilience Testing**

**ICT Third Party Management**

**Oversight of Critical ICT Vendors**

# DORA will apply to **financial entities (FE)**

**WHO**

- **credit institutions**,
- payment institutions,
- e-money institutions,
- **investment firms**,
- cryptoasset service providers (authorised under MiCA) and issuers of asset-referenced tokens,
- central securities depositories,
- central counterparties,
- trading venues,
- trade repositories,
- managers of alternative investment funds and management companies,
- data reporting service providers,
- **insurance and reinsurance undertakings**,
- insurance intermediaries,
- reinsurance intermediaries and ancillary insurance intermediaries,
- institutions for occupational retirement pensions,
- credit rating agencies,
- administrators of critical benchmarks,
- crowdfunding service providers and
- securitization repositories

# Types of institutions that fall outside the scope

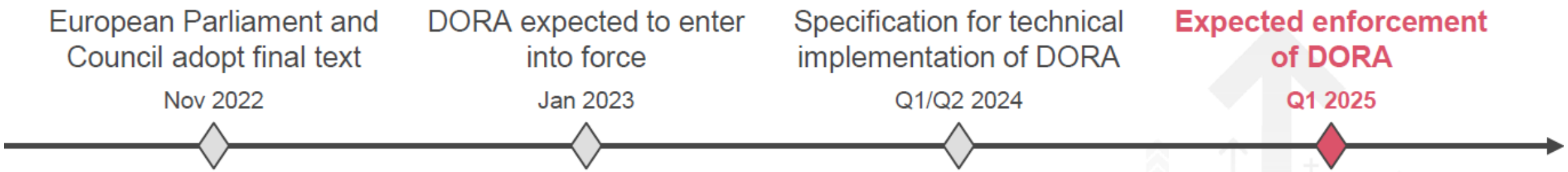
WHO

- Managers of alternative investment funds referred to in Article 3(2) of Directive 2011/61/EU – small scope AIFM
- Insurance and reinsurance undertakings referred to in Article 4 of Directive 2009/138/EC1
- Institutions for occupational retirement provision which operate pension scheme which together do not have more than 15 members in total
- Natural or legal persons exempted from the application of Directive 2014/65/EU pursuant to Articles 2 and 3 of that Directive
- Insurance intermediaries, reinsurance intermediaries and ancillary insurance intermediaries which are microenterprises, small or medium-sized enterprises
- Post office giro institutions as referred to in Article 2(5), point (3), of Directive 2013/36/EU.
- Member States may exclude from the scope of DORA certain entities (entities referred to in Article 2(5), points (4) to (23), of Directive 2013/36/EU that are located within their respective territories. )
- Microenterprises are excluded form the majority of obligations.

# DORA timeline

**WHEN**

- 09/2020: The first draft of DORA.
- 10/11/2022: DORA (the final text) is adopted by the EU parliament.
- Q1 2023: DORA will come into effect
- Q1 2025: DORA will apply to in-scope institutions and companies.




Source:
https://www.pwc.de/de/cyber-security/pwc-germany-dora-overview.pdf

# ICT Risk Management

- FEs should have in place internal governance and control frameworks to ensure an effective and prudent management of all ICT risks.
- Management body has "full responsibility" in adopting, managing and monitoring the **digital operational resilience strategy**; managing ICT risks; and reviewing and approving the corporate policy on the use of ICT Third Party Providers (TPPs).
- FEs should:
  - establish **ICT risk management framework** that should cover the following areas: identification, protection and prevention, detection, response and recovery, learning and evolving, communication.
  - identify their "critical or important functions" (CIFs) and map their related assets and interdependencies.
  - articulate their risk appetite for disruption to critical or important functions.
  - conduct business impact analyses based on "severe business interruption" scenarios.
- Simplified ICT Risk Management framework for some institutions.

European Banking Authority's (EBA) guidelines on ICT security and risk management (EBA/GL/2019/04)

# ICT Incident Reporting

- FEs should establish and implement:
  - ICT-related incident management processes to detect, manage and notify ICT-related incidents
  - early warning indicators as alerts.
- FEs must classify ICT-related incidents and determine their impact based on pre-established criteria.
- Mandatory notification by FEs to NCAs on major ICT related incidents (3-part notification template: initial report, intermediate report and final report).
- Voluntary notification of significant cyber threats to the relevant CAs (relevant to the financial system, service users or clients).

EBA's Guidelines on major incident reporting under PSD2 (EBA/GL/2021/03)

# Digital Operational Resilience Testing

- FEs must have a sound and comprehensive digital operational resilience testing programme → assessing preparedness for handling ICT-related incidents, identifying weaknesses, efficiencies or gaps in the digital operational resilience and prompt implementation of corrective measures.
- It should include a range of assessments, tests, methodologies, practices, and tools.
- Tests must be performed by independent (internal or external) testers.
- All critical ICT systems and applications shall be tested at least on a yearly basis.

## TLPT

- Requirements for testers for the deployment of threat led penetration testing (TLPT): have to possess the highest suitability and reputability and be certified by an accreditation body in a Member State or adhere to formal codes of conduct or ethical frameworks.
- NCAs designate FEs that are required to perform TLPT. Significant FEs should perform TLPT at least once every 3 years. TLPTs are performed in live environment.
- Vendors supporting CIFs should be included in advanced testing exercises (TLPTs).
- TLPT framework will probably similar to the TIBER-EU framework.

European Central Bank's (ECB) TIBER-EU framework

# ICT Third Party Risk Management

- FEs are required to manage ICT third party risk as an integral component of ICT risk within their ICT risk management framework.
- FEs should maintain a Register of Information in relation to all contractual arrangement on the use of ICT services provided by ICT third party service providers (TPPs). NCAs will collect those registers.
- Intragroup provision of services is subject to the framework.
- Focus on supply chains.
- Wide general principles that focus on the assessments before entering into a contractual arrangements, reasons for service termination and exit strategies.

EBA Guidelines on o utsourcing arrangements (EBA/GL/2019/02)

# Oversight of Critical Third Party Providers (CTPPs)

- World's first third-party oversight regime initiative in the financial sector.
- CTPPs will have to have in place comprehensive, sound and effective rules, procedures, mechanisms and arrangements to manage the ICT risks which they may pose to FEs.
- It is expected that certain categories of providers, such as cloud computing service providers who provide ICT services to FEs, will be designated as CTPPs.
- Expressly excluded from the designation:
  - FEs providing ICT services to other FEs,
  - ICT intra-group service providers and
  - ICT TPPs providing services solely in one MS to FEs that are only active in that MS.
- FEs will only be permitted to make use of the services of a third-country CTPP if such provider establishes a subsidiary in the EU within 12 months following its designation as a CTPP.
- Penalties up to 1% of the average daily worldwide turnover, imposed on a daily basis until compliance is achieved and for no more than a period of six months.

HOW

Implementation shall be in accordance with the principle of **proportionality**, taking into account size, nature, scale and complexity of services, activities and operations and the overall risk profile.

# The details will be prescribed via numerous level-2 documents/standards/regulations

**HOW**

The documents that have to be published in **Q1 2024*:**

- RTS on ICT incident classification procedures and cyber threats
- RTS on the level of detail required in third-party provider management strategies (TPPs)
- RTS on the additional elements of the ICT risk management framework
- ITS on the Register of information relating to contractual agreements with suppliers in the ICT field

The documents that have to be published in **Q2/Q3 2024*:**

- RTS on reporting serious ICT and cyber incidents to authorities
- RTS on scope and additional elements for advanced testing

* Publication of drafts of the documents and public consultations will start earlier

# The details will be prescribed via numerous level-2 documents/standards/regulations

**HOW**

The documents that have to be published in **Q2/Q3 2024*** (cont'd)**:**

- RTS on key contractual arrangements for the subcontracting of functions/services in support of critical or important functions
- RTS on the appointment of members of a Joint Examination Team
- RTS on the information to be provided by a CTPP to supervisory authorities
- European Commission Delegated Act on the Designation of Critical service Providers (CTPP)
- European Commission Delegated Act on Supervisory Fees for Critical service Providers (CTPP)

The documents that have to be published in **Q1 2025*:**

- ESA report on the creation of a central EU hub for incident reporting

* Publication of drafts of the documents and public consultations will start earlier

# Sources and further reading


- Apex: *Digital Operation Resilience Act* , https://www.apexgroup.com/media/sz4djcpk/apex-group-global-reg-tracker-dora-final.pdf
- Clifford Chance: *DORA: What The New European Framework for Digital Operational Resilience Means for Your Business*, *https://www.cliffordchance.com/content/dam/cliffordchance/briefings/2022/11/dora-what-the-new-european-framework-for-digital-operational-resilience-means-for-your-business.pdf*
- Deloitte: *EU Digital Operation Resilience Act passed: implications for the financial sector* , https://www2.deloitte.com/content/dam/Deloitte/it/Documents/risk/digital-operation-resilience-act-deloitte-eng.pdf
- PwC: *Digital Operation Resilience Act (DORA): Overview for financial entities and ICT third parties*, https://www.pwc.de/de/cyber-security/pwc-germany-dora-overview.pdf

# DORA will set the regulatory focus on four key areas

## 1 ICT Risk Management

- Laying out a detailed IT risk management framework in alignment with the business strategy and objectives
- Defining a digital resilience strategy
- Setting the focus on Business Continuity and Disaster Recovery

## 2 Digital Operational Resilience Testing

- Annual testing of all critical ICT systems
- Advanced threat-led penetration testing every 3 years (in the likes of TIBER-EU)
- Collaboration with ICT third-party providers

## 3 ICT-related Incident Reporting

- Reporting of cyber incidents – submission of initial, intermediate and final reports
- Implementing a root-cause-analysis following cyber incidents
- Identifying and reporting required improvements

## 4 ICT Third Party Risk Management

- Reporting the complete outsourcing register (incl. intra-group services)
- Reporting of changes in outsourcing activities
- Assessment of ICT concentration risk and sub-outsourcing arrangements
- Only sourcing of critical third-party service providers with an EU entity

**Source**:
https://www.pwc.de/de/cyber-security/pwc-germany-dora-overview.pdf

# Acronyms and abbreviations

| | |
|---|---|
| **CA** | Competent Authority |
| **CER** | Critical Entity Resilience Directive |
| **CIF** | Critical or Important Function |
| **CRD** | Credit Requirements Directive |
| **CTPP** | Critical Third Party Service Provider |
| **DFS** | Digital Finance Strategy |
| **EBA** | European Banking Authority |
| **ECB** | European Central Bank |
| **ESAs** | European Supervisory Authorities |
| **FE** | Financial Entity |
| **GDPR** | General Data Protection Regulation |

| | |
|---|---|
| **ICT** | Information and Communication Technology |
| **ITS** | Implementing Technical Standard |
| **MS** | Member State |
| **NCA** | National Competent Authority |
| **NIS2** | Network and Info. System Security Directive |
| **NISD** | Network and Information Systems Directive |
| **PSD2** | Payment Services Directive 2 |
| **RTS** | Regulatory Technical Standard |
| **TIBER** | Threat Intelligence-based Ethical Red-teaming |
| **TLPT** | Threat Led Penetration Testing |
| **TPP** | Third Party Service Provider |