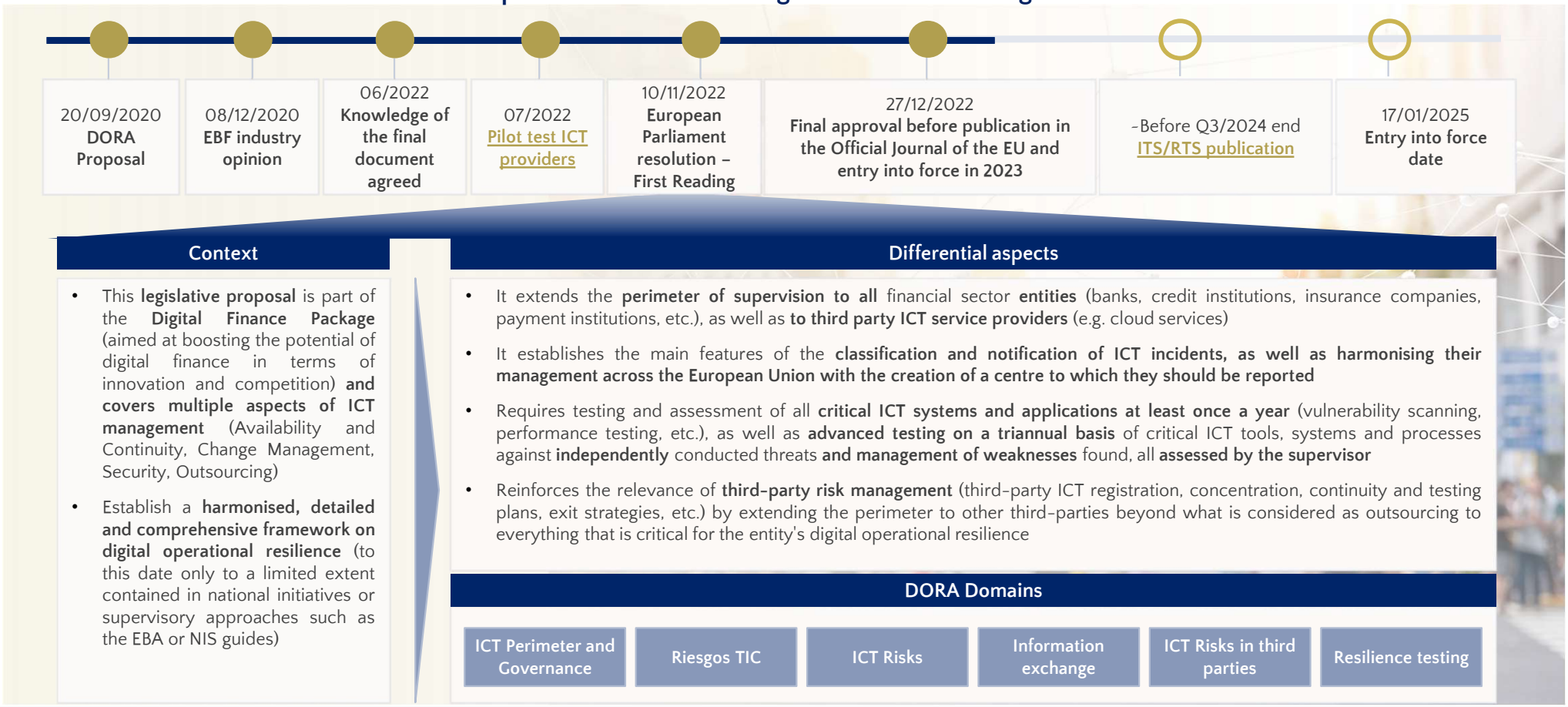
Technology Risks and Cybersecurity

The DORA challenge: main impacts and market gaps

1. DORA Understanding – Regulation Timeline, Context and Main Objectives

In this sense, DORA details many of the requirements established in the EBA Guidelines (ICT and Outsourcing), adding new requirements or reinforcing some of the existing ones



Context

- This **legislative proposal** is part of the **Digital Finance Package** (aimed at boosting the potential of digital finance in terms of innovation and competition) **and covers multiple aspects of ICT management** (Availability and Continuity, Change Management, Security, Outsourcing)
- Establish a **harmonised, detailed and comprehensive framework on digital operational resilience** (to this date only to a limited extent contained in national initiatives or supervisory approaches such as the EBA or NIS guides)

Differential aspects

- It extends the **perimeter of supervision to all** financial sector **entities** (banks, credit institutions, insurance companies, payment institutions, etc.), as well as **to third party ICT service providers** (e.g. cloud services)
- It establishes the main features of the **classification and notification of ICT incidents, as well as harmonising their management across the European Union with the creation of a centre to which they should be reported**
- Requires testing and assessment of all **critical ICT systems and applications at least once a year** (vulnerability scanning, performance testing, etc.), as well as **advanced testing on a triannual basis** of critical ICT tools, systems and processes against **independently** conducted threats **and management of weaknesses** found, all **assessed by the supervisor**
- Reinforces the relevance of **third-party risk management** (third-party ICT registration, concentration, continuity and testing plans, exit strategies, etc.) by extending the perimeter to other third-parties beyond what is considered as outsourcing to everything that is critical for the entity's digital operational resilience

DORA Domains

ICT Perimeter and Governance	Riesgos TIC	ICT Risks	Information exchange	ICT Risks in third parties	Resilience testing

2. DORA Understanding – Domains of regulation

The regulation is divided into six domains, the main impacts are detailed below

ICT Perimeter and Governance

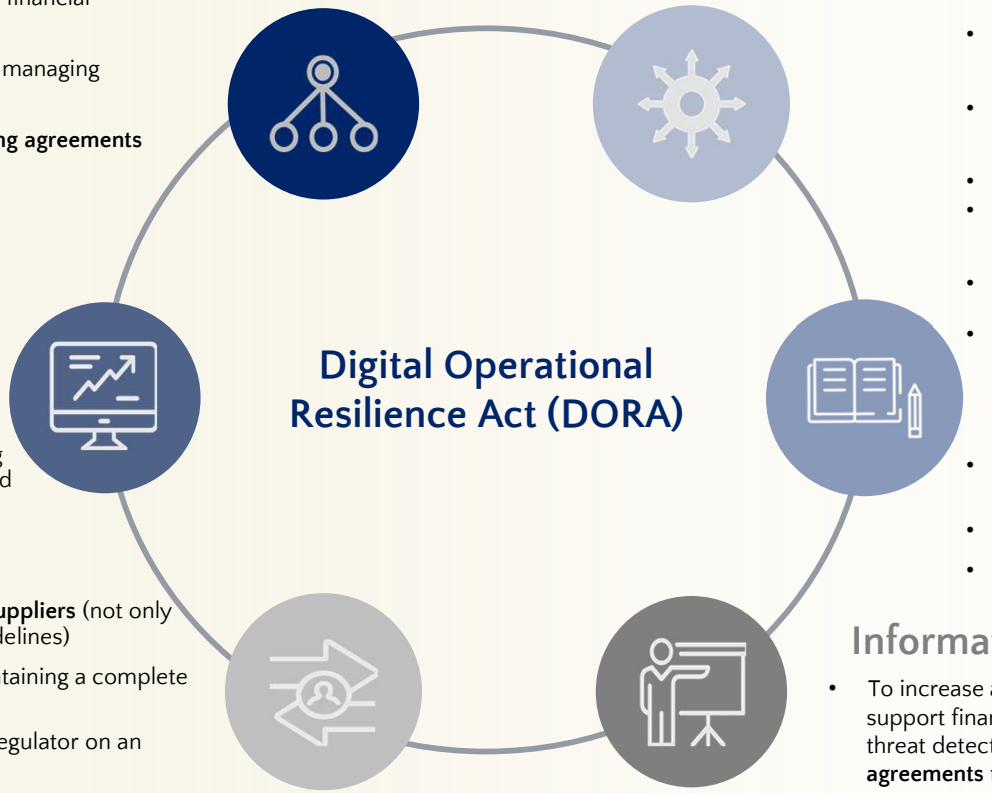
- Extension of the scope **of application** to any financial institution, including ICT service providers.
- Responsibilities of the **Management Body** in managing operational resilience
- Identification of a role in charge of **monitoring agreements with third parties** for ICT services.

Resilience Testing

- **Annual testing** of all critical ICT systems and applications (vulnerabilities, code analysis, performance, capacity, etc.)
- **Advanced** threat lead penetration **testing** of critical functions and services, validated by supervisory authorities
- Dedicating sufficient **resources** and ensuring that conflicts of interest (between design and test execution) are avoided

ICT Risks in third parties

- Extension of the **perimeter to all high-risk suppliers** (not only those considered as outsourcing in EBA guidelines)
- Development of an **information registry** containing a complete overview of all ICT third parties
- Reporting of **changes to the register** to the regulator on an annual basis
- **ICT concentration risk** assessment



ICT Risks

- Existence of an **internal governance and control framework** for ICT risks
- **Existence of adequate protection measures**: access control model and profiling, network segmentation, system patching, etc.
- Identification and classification, according to criticality, of ICT support **functions and assets** and their interdependencies with third parties
- Continuous identification of **sources of risk**
- **Existence of a risk-based backup policy and the development of recovery and response strategies**
- **Annual** specific **risk assessment of** all legacy ICT systems
- Developing **specific** digital resilience **awareness and training programs**

Reporting of ICT Incidents

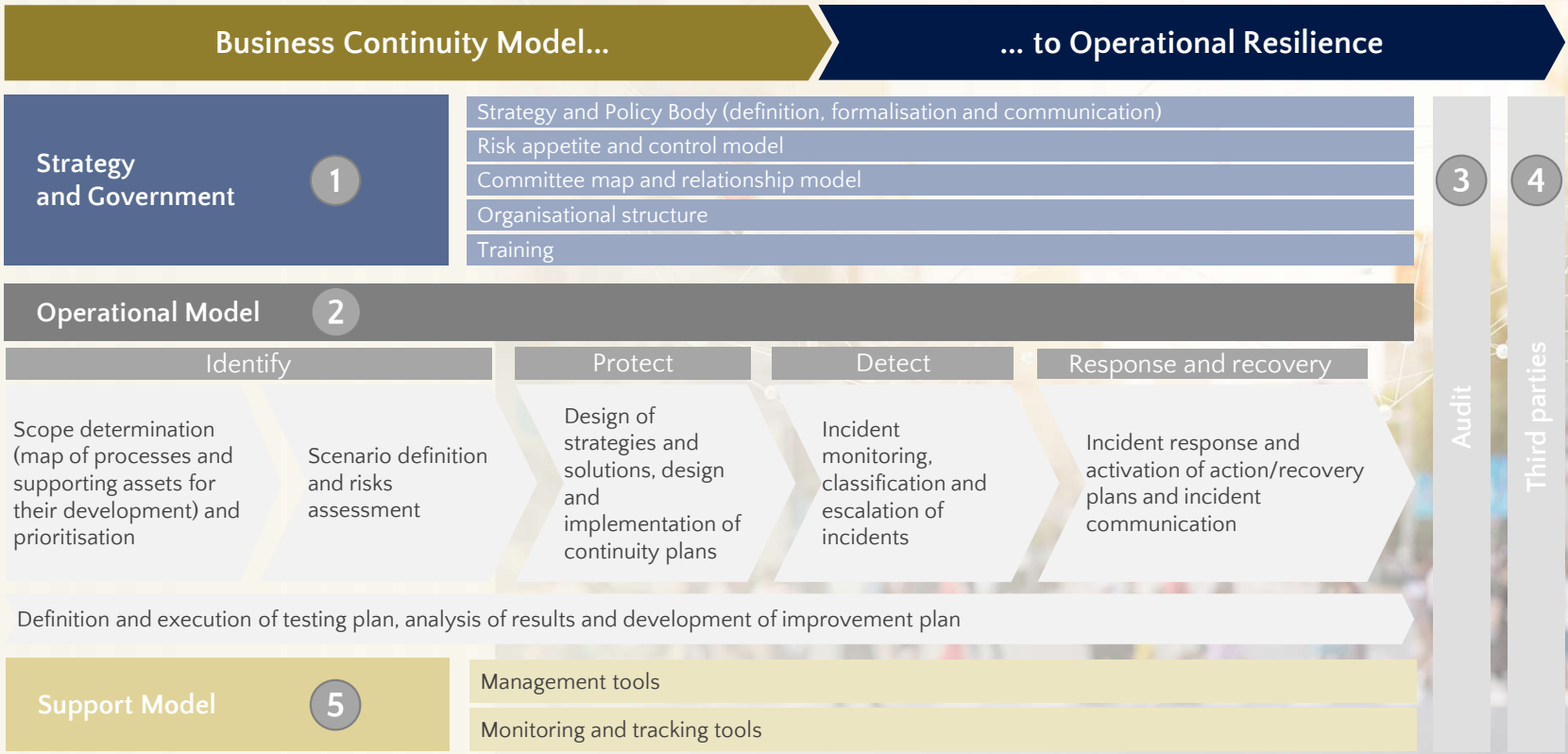
- Mechanism to **monitor and follow up incidents** until causes are eradicated
- Specific criteria for **incident classification**
- Extending the reporting perimeter to **operational or payment-related incidents**

Information exchange

- To increase awareness of ICT risks, minimise their spread, support financial institutions' defensive capabilities and threat detection techniques, the regulation calls for **agreements to exchange information on cyber threats**

3. DORA Implementation – Control Framework Evolution

These requirements have an impact on the technological risk management and resilience frameworks that institutions are evolving, taking into account five main axes



4. *DORA* Gaps – *Hot Topics*

The following is a summary of some of the main issues that are receiving the most attention in DORA compliance projects

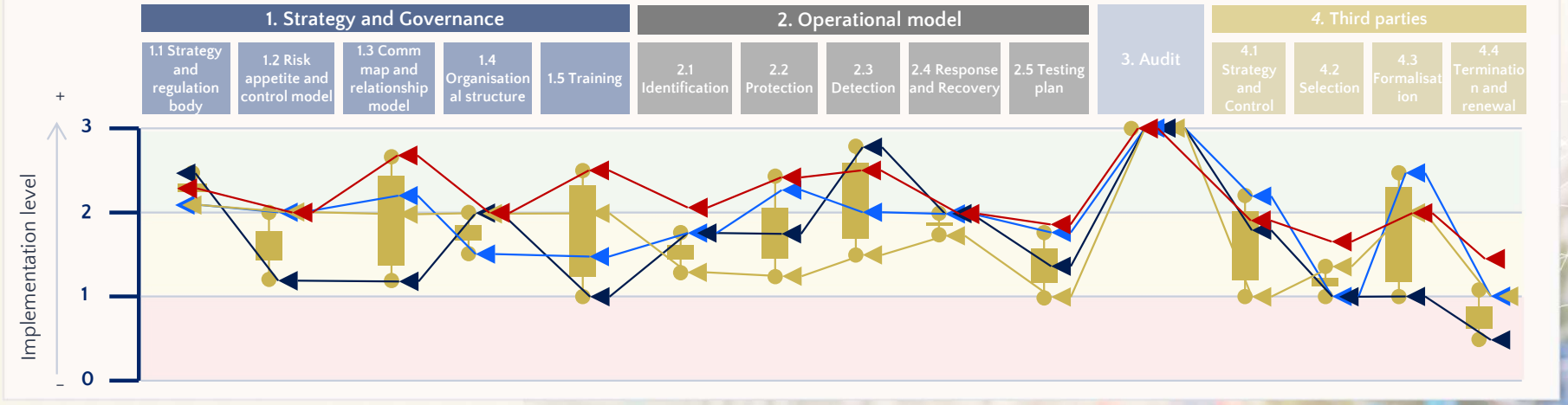
01. Strategy and governance	• Evaluation of the **extension of the perimeter**, with a focus on how to incorporate a **tiering criterion** and establish the degree of **deployment** of the **ICT risk management framework on the different companies** in a proportional manner. • Review of the **ICT risk appetite framework** to update and/or incorporate indicators and thresholds focused on digital operational resilience.
02. Operating model	• Review of **asset inventories**, including their linkage to business and support processes/functions, as well as the determination of the criteria for **classifying those that are critical** (taking into account the principles of confidentiality, availability and integrity defined in the EBA Guildelines). • Discussion on how to establish a **quantification methodology** to estimate the **potential losses** associated with **critical events** (generally of low probability and high impact). • Incorporation or **reinforcement of measures** that require a relevant effort, whether focused on **protection** (e.g. network segmentation, access control) or **response/recovery** (e.g. backups, recovery and response strategies). • Discussion on how to establish a **yearly testing plan** with annual periodicity, on critical ICT assets and applications and consider all the required testing pool (open source analysis, penetration testing, questionnaires and scanning of software solutions, source code review...). Determination of roles and responsibilities to avoid conflicts of interest between those who design and those who execute the tests.
03. Audit	• It is not being an area of special attention
04. Third parties	• Extension of current **outsourcing management models to ICT Third Parties** under the scope of DORA (regulatory body, contractual frameworks, monitoring/audit models, concentration analysis...). • Updating and extending **ICT vendor inventories** to match regulatory/supervisory expectations • Review and reinforcement of **continuity plans and testing, as well as exit strategies** with suppliers

5. DORA Status – DORA Overview in the Industry

T1 T2 T3 T4 Max Avg. value Min Avg. value

Taking into account these axes of analysis, a partial degree of compliance with DORA requirements is observed in the industry in Tier 1 and Tier 2 financial institutions

Benchmark results by framework block



Hot topics

- **In the perimeter extension,** it may take into account a tiering criteria and establish the degree of deployment of the ICT risk management framework over the different companies on a proportional basis
- Establishing a **methodology that identifies critical ICT systems and applications as well as critical functions and services** (taking into account the principles of confidentiality, availability and integrity as defined in the EBA Guidelines)
- Defining **a regular testing plan** on an annual basis, on critical ICT assets and applications and that plan takes into account all the required testing pool (open source code analysis, penetration testing, questionnaires and scanning of software solutions, source code review...). Determination of roles and responsibilities
- Establishing a **quantification methodology** to estimate the potential losses associated with critical events (generally of low probability and high impact)

Annex:

A1 | Pilot test on ICT suppliers

A1. Pilot test on ICT suppliers – Context and key elements

After the agreement on the final text of DORA, ESAs kicked off in July an aggregated exercise to assess the general context of ICT's service suppliers from an inspection perspective. There are already some conclusions and possible actions to be considered

07/2022
Pilot Test communication

09/2022
Webinar & FAQs

10/2022
Survey delivery

Exercise sample

This exercise is aimed at a sample of entities of different sectors. Its main objective is to gather information of TIC'S suppliers' services in terms of concentration and dependencies.

Perimeter

- **The application is done at an economic group level** (consolidated level)
- **Information is requested for each contract** with each ICT Third Party in each entity of the group.
- **The preliminary taxonomy of services provided by "Third Parties" confirms that the scope** includes not only outsourcing activities, but **also software development and licensing, data centres and security services.**
- **Intra-group agreements and joint ventures are included.**
- Right now, **no materiality threshold is indicated.**

Information Requested

Identification	• **Identification of the entities of the contract** (signatory and users) • **Supplier identification** (company and group)
Contracted functions	• **List of services provided** (e.g. software development, DCs, Sec, aaS) • **Criticality of each service** according to the applicable sectoral definition
Risk Assessment data	• **Level of dependency and exit strategy parameters** • **Legal aspects: Applicable law and subcontracting controls**

Pilot Exercise

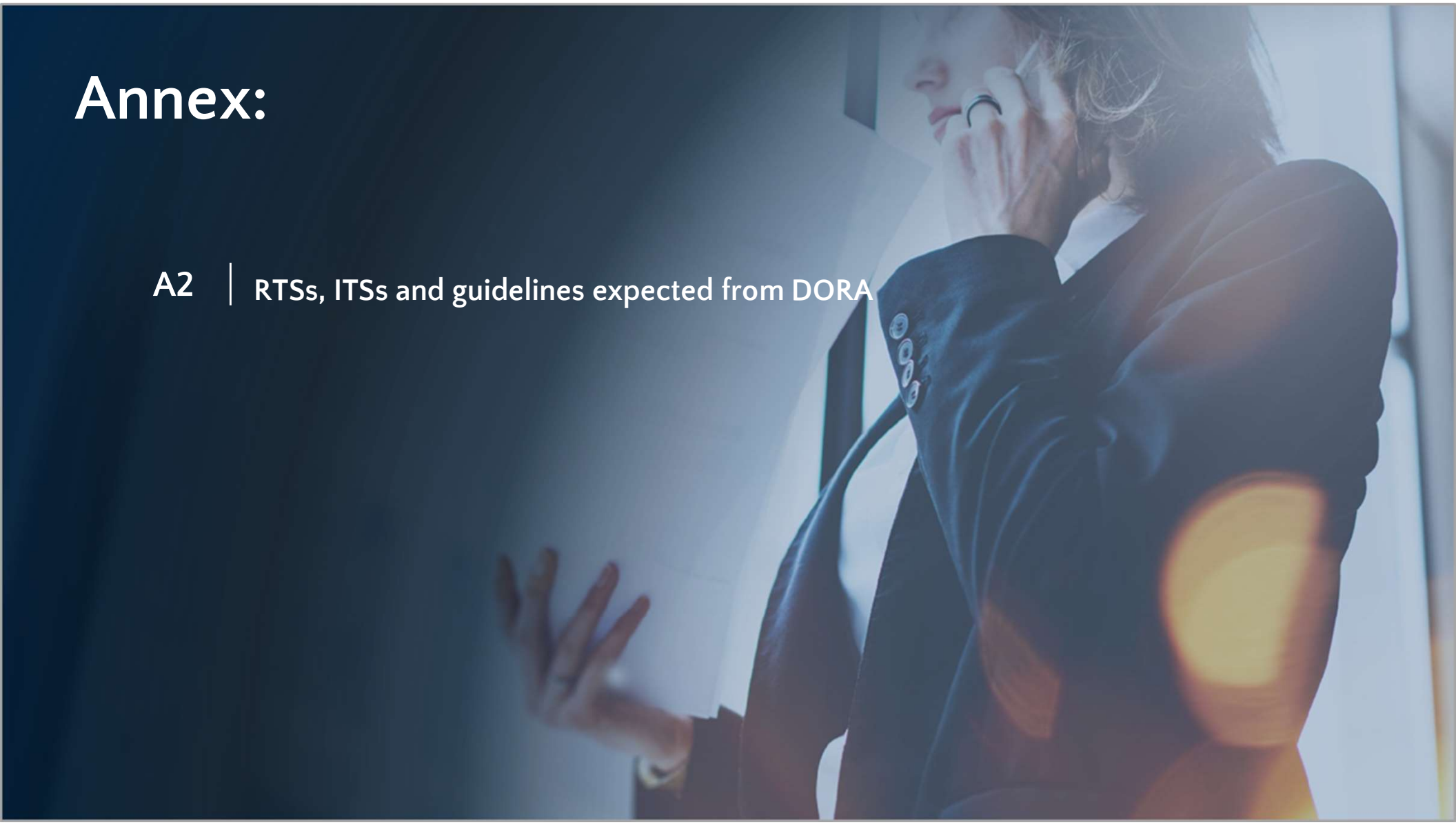
DORA will require an annual submission of a third party ICT register, therefore, this exercise is a first approximation of the information requirements that will be requested.

Conclusions of the Exercise

- **The final report to be submitted on a recurring basis in 2025 will be different**, but the current request gives some important indications on the level of detail that will be requested
- **Obtaining this level of detail in large groups may require two types of actions:**
  - Identification of contracts
  - Reviewing existing recruitment processes at group level to ensure that the information register is up to date.
- **The definition of** credible and **feasible exit strategies and the monitoring of subcontracting chains will be essential** to demonstrate that the risk with third parties is under control. A review of the minimum requirements for contracts with ICT suppliers is advisable.
- **The mentioned review should take into account not only the specific aspects of the application, but also the additional requirements included in DORA** to make such contracts progressively compliant.

Annex:

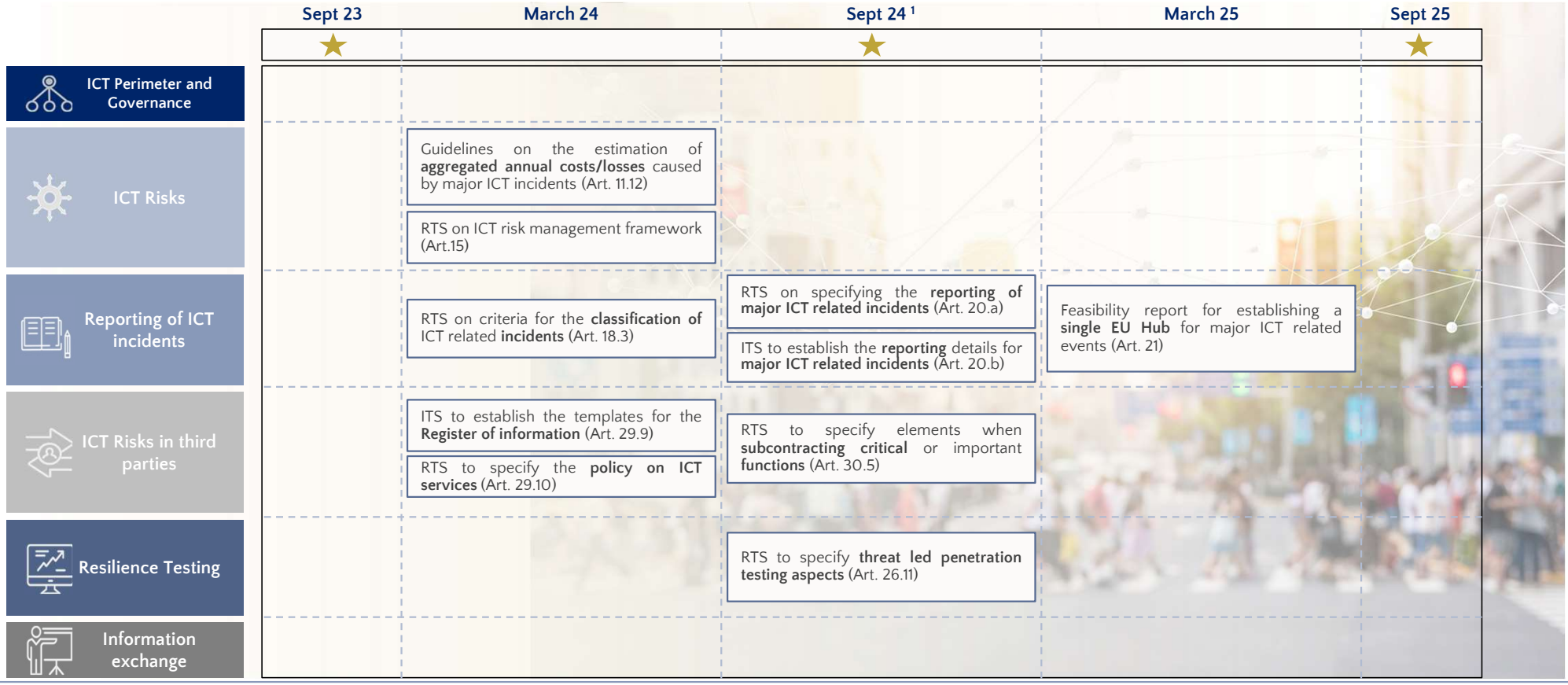
A2 | RTSs, ITSs and guidelines expected from DORA



A2. RTSs, ITSs and guidelines expected from DORA– Timeline

★ ESRB recommendation

The competent authorities will distribute over the next 18 months a series of RTSs, ITSs, Guidelines, etc. listed below to complement various aspects and ensure a homogeneous implementation among the different European entities affected by the regulation



[1] GL on cooperation between ESAs and Competent Authorities in relation to the structure of supervision (Art.32.7) and RTS to specify information on supervisory conduct (Art. 41) in relation to the section of the framework for supervision of third-party providers