Digital Operational Resilience Act

T. Plomteux

Febelfin webinar | 13 January ’23

Banque Nationale de Belgique / Bank van België
Eurosystem

FOR DISCUSSION ONLY

Disclaimer

This slideshow reflects my current understanding of and some personal ideas regarding DORA. It should not be construed as an official statement by the National Bank of Belgium.

Agenda

- Intro + NBB organisation ~~r IT/cyber risk supervision~~
- DORA
- Overview content
- Negotiations and outcome
- Implications ESAs/NCAs/MSs
- ~~Impact f ncial entities~~
- Q&A

Shortened version

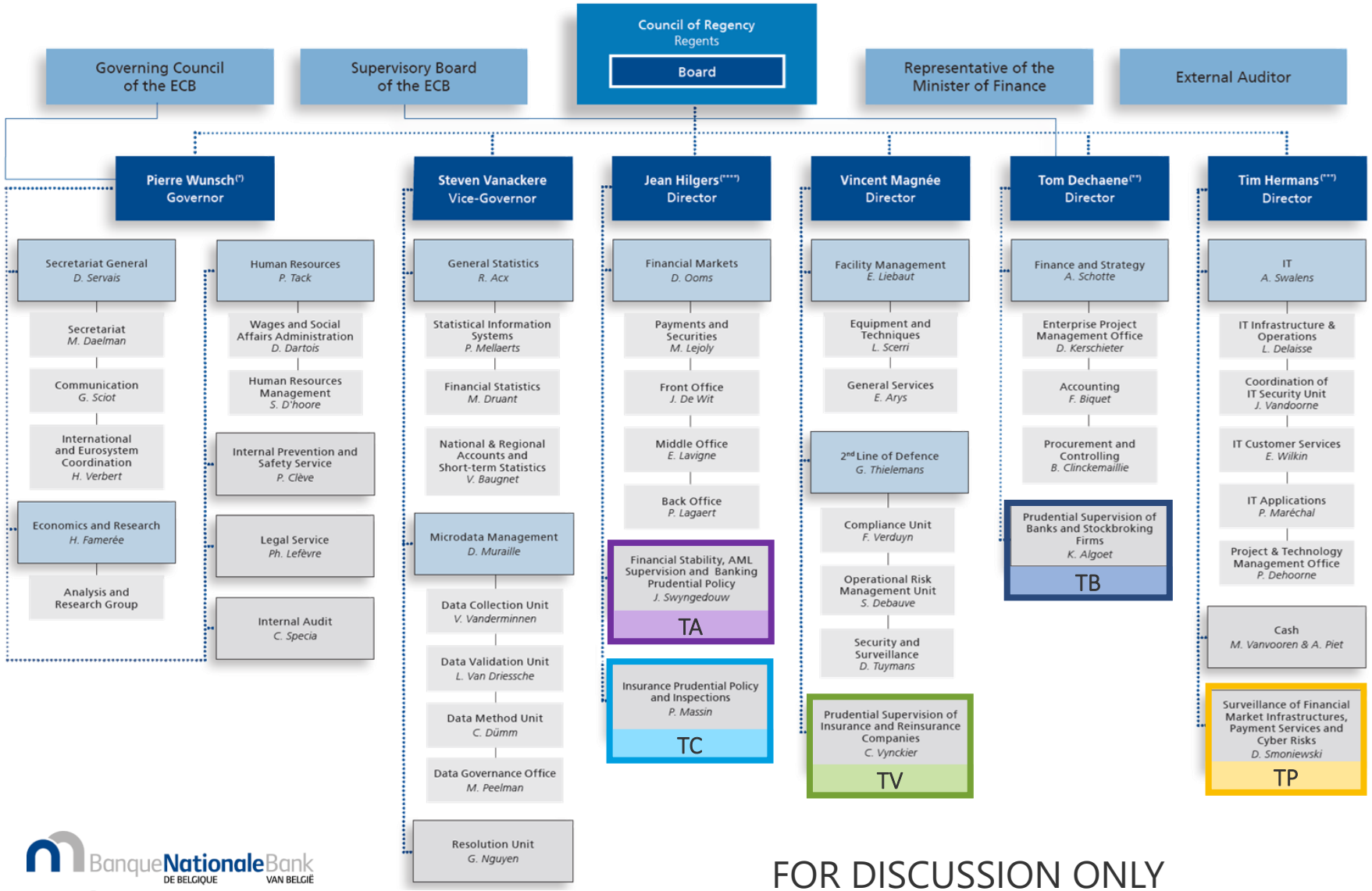
Intro + NBB organisation for IT/cyber risk supervision

Update on the Digital Operational Resilience Act

Banque Nationale de Belgique / Bank van België
Eurosystem

FOR DISCUSSION ONLY

IT/cyber supervision in the NBB organisational chart



TA Financial stability, AML supervision & banking prudential policy

TB Prudential Supervision of Banks & Stockbroking Firms

TC Insurance Prudential Policy & Inspections

TV Prudential Supervision of Insurance & Reinsurance Companies

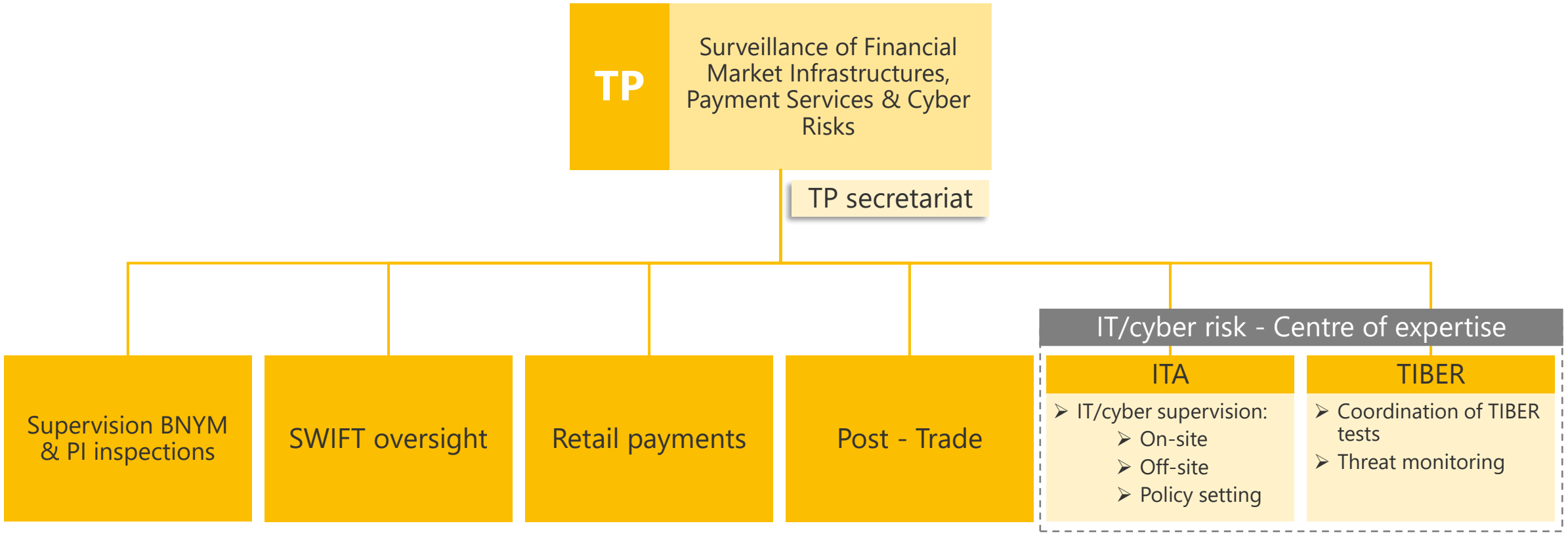
TP IT/cyber subject matter experts provide expertise/know-how to other prudential services for IT related matters

TP Surveillance of Financial Market Infrastructures, Payment Services & Cyber Risks

BanqueNationaleBank DE BELGIQUE VAN BELGIË
Eurosystem

FOR DISCUSSION ONLY

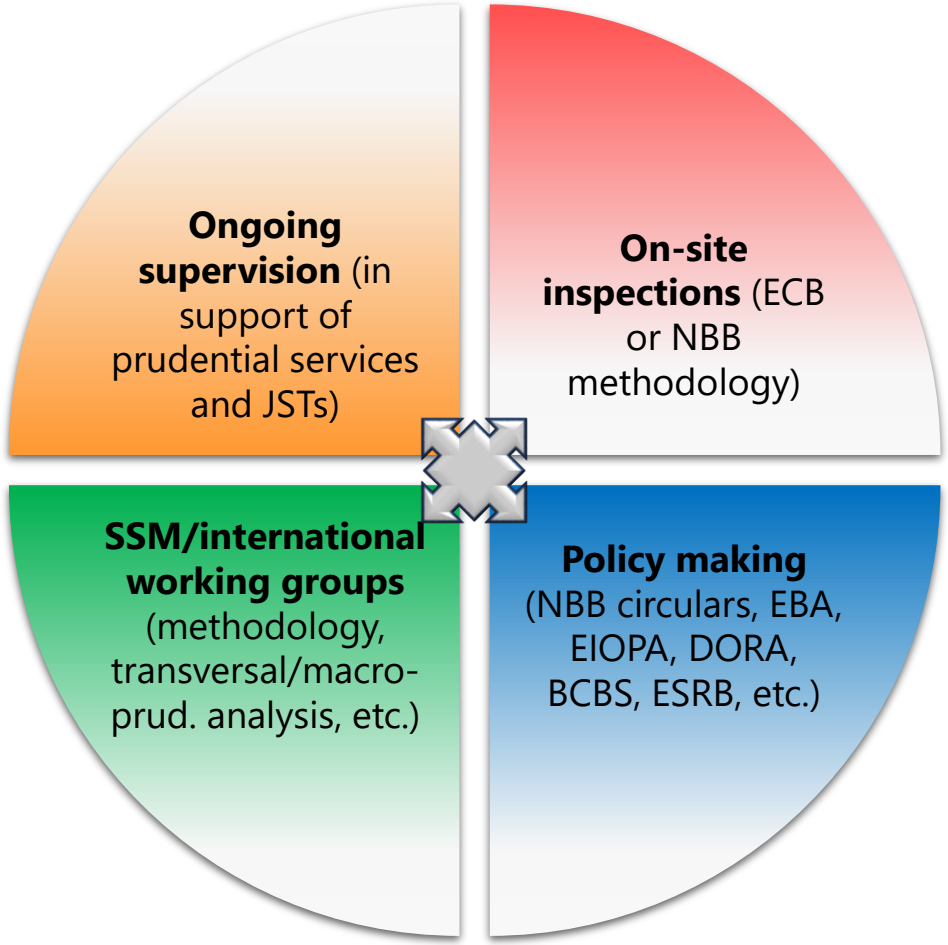
Organisation of the TP service



FOR DISCUSSION ONLY

IT/cyber supervision in the NBB

TP-ITA team core tasks



- **IT expert centre**
- Currently 10 FTE
- Supporting **all prudential services**
- Centralising IT expertise realizes **considerable economies of scale**:
  - Flexible risk-based allocation of resources
  - Knowledge sharing
  - Level playing field (within Belgium)
- Areas of expertise: **information security**, **IT continuity**, **IT outsourcing/cloud computing**, IT project risks, IT complexity, Fintech, data quality

The TIBER-BE national implementation

TIBER-BE team core tasks

TIBER-BE engagements

TIBER-BE Community

Continuous improvement efforts

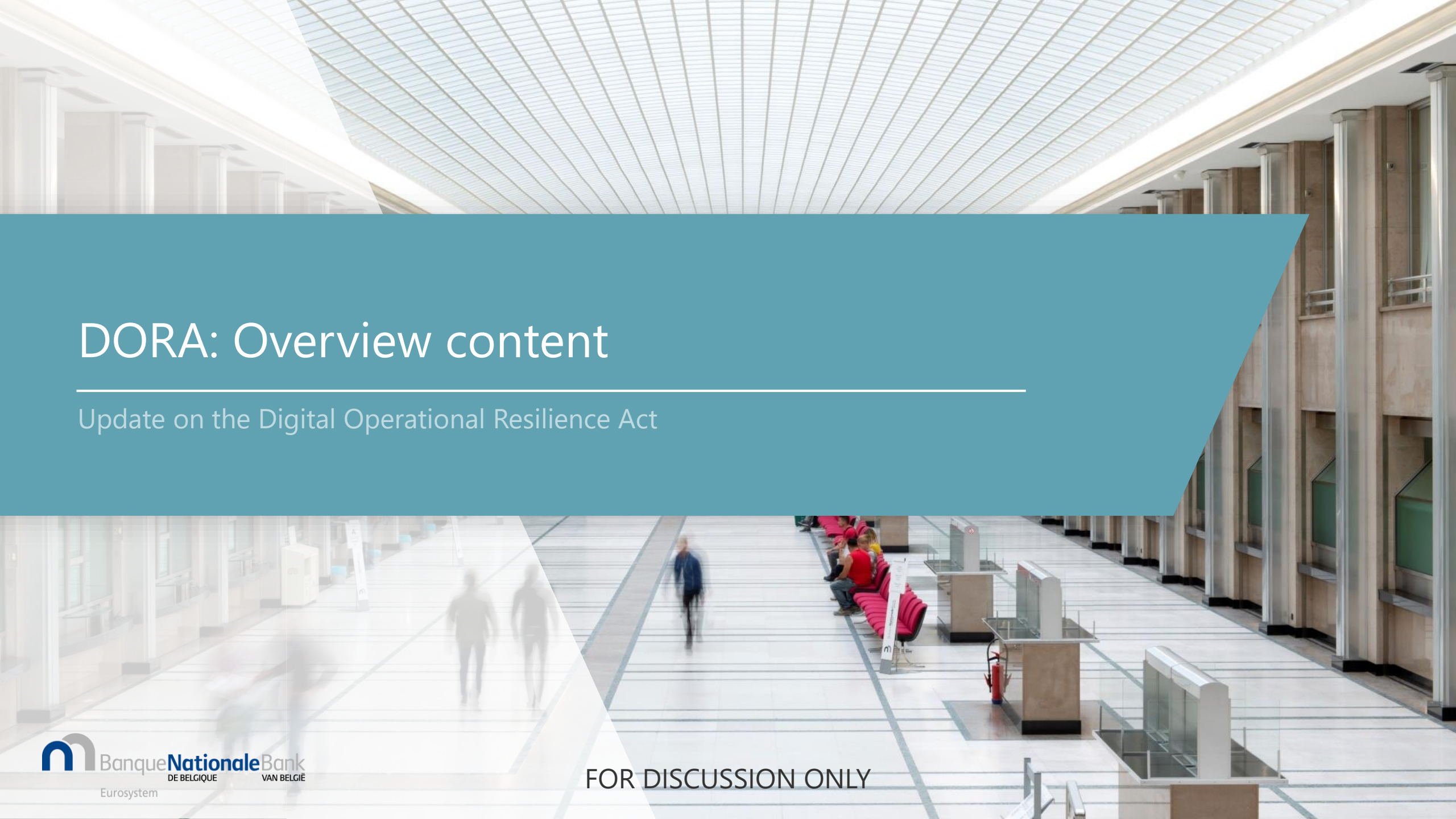
Governance & reporting

TIBER knowledge centre & TIBER-EU/XX collaboration

Cyber threat intelligence

Training

Participation/contribution to/for various (inter)national and internal fora (for example on cyber intel sharing, DORA, ECRB, IT risk …)



DORA: Overview content

Update on the Digital Operational Resilience Act

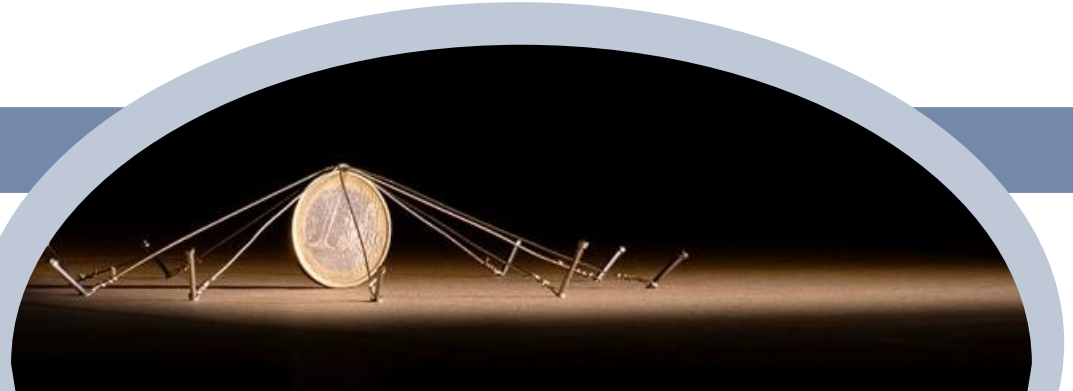
Banque Nationale de Belgique / Bank van België
Eurosystem

FOR DISCUSSION ONLY

DORA background & context

- Part of **Digital Financial Package** (DG-FISMA – 24/09/'20)
  - Enabling **benefits of digitalization** by controlling **risks** (e.g. crypto assets, DLT …)
  - Ensure a safe financial system **across** its **sub-sectors**

- **EU regulation** (<> EU directive)
  - **Avoid diverging approaches** by instating common rules on digital operational resilience
  - A **broad range** of **financial entities** subject to requirements
  - **Lex specialis** to horizontal NIS 2 Directive
  - 27/12/'22 version text: **link**



DORA chapters

(more detail in annex)

I - General Provisions

II - ICT Risk Management

III - ICT-related incidents

IV - Digital operational resilience testing

V - Managing of ICT third-party risk

VI - Information sharing arrangements

VII-IX - Competent authorities, Delegated acts, Transitional and final provisions

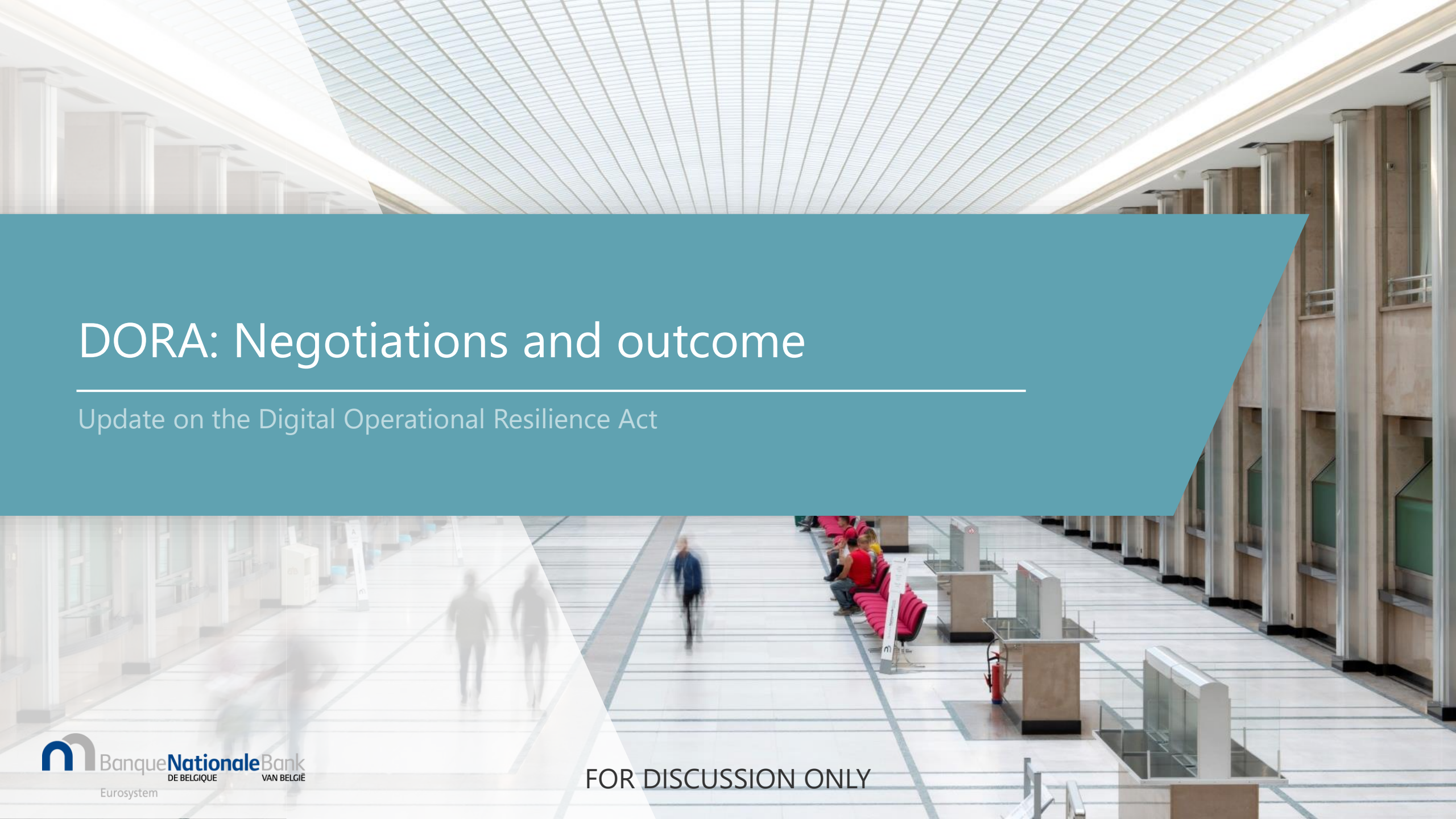
BanqueNationaleBank DE BELGIQUE VAN BELGIË
Eurosystem

DORA institutions in scope

a. **Credit institutions***
b. **Payment institutions/account info SPs***
c. **Electronic money institutions***
d. **Investment firms***
e. Crypto-asset SPs etc.
f. **Central securities depositories**
g. Central counterparties
h. Trading venues
i. Trade repositories
j. Managers of alternative investment funds*
k. Management companies
l. Data reporting service providers
m. **Insurance & reinsurance undertakings** *
n. Insurance and reinsurance intermediaries*
o. Institutions for occupational retirement provision*
p. Credit rating agencies
q. Administrators of critical benchmarks
r. Crowdfunding SPs
s. Securitisation repositories
t. ICT third-party providers*

Bold : most relevant in NBB context

(*) with some exceptions and some under a lighter regime



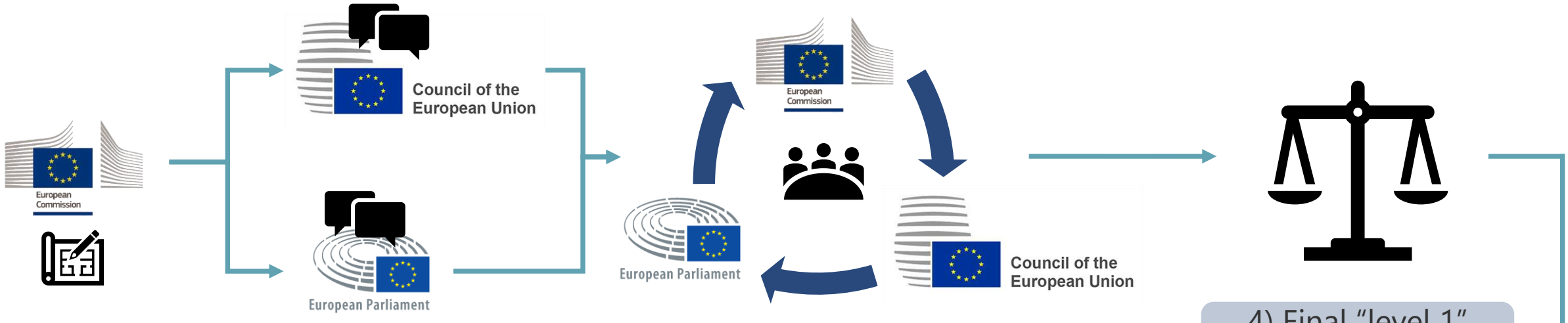
DORA: Negotiations and outcome

Update on the Digital Operational Resilience Act

Banque Nationale de Belgique / Bank van België
Eurosystem

FOR DISCUSSION ONLY

Process & timeline



1) Proposal

24/09/'20

2) Compromises

24/11/'21 & 1/12/'21

3) Trialogues

25/01/'22 - 10/05/'22

4) Final "level 1" published

27/12/'22

5) Entry into force

17/01/'23

6a) RTS(s) & ITS(s)*

See annex

6b) Application date

17/01/'25

* Regulatory & Implementation Technical Standards ("level 2")

DORA preliminary outcome for scope

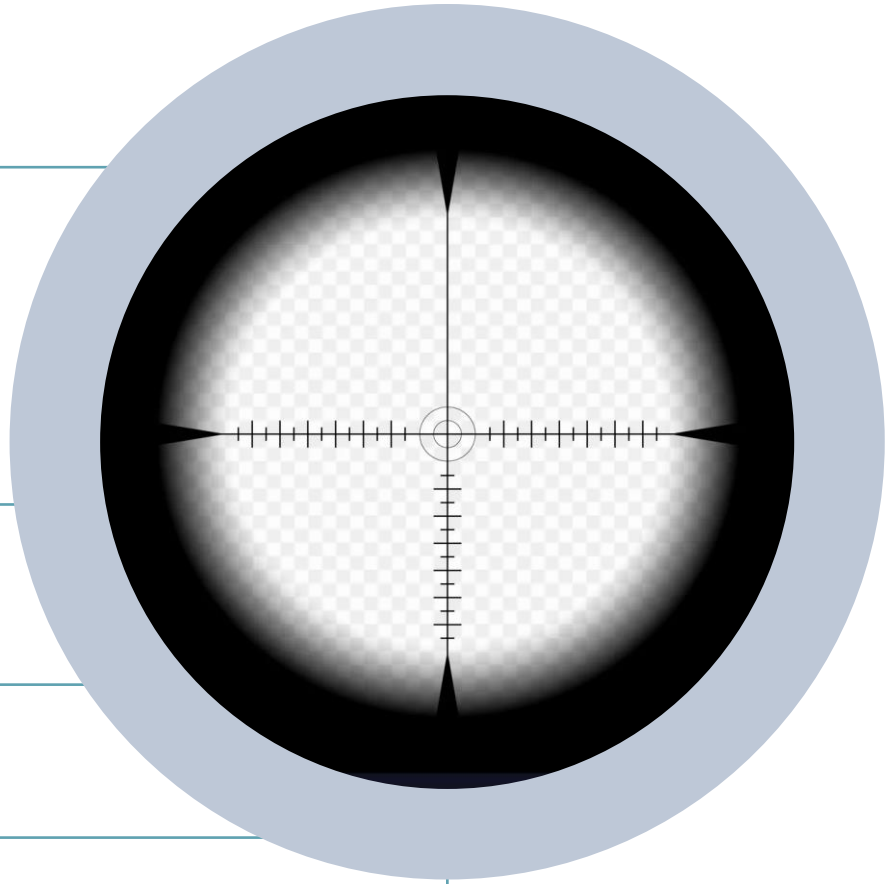
Payment systems and **payment-processing** activities
→ out-of-scope
- COM to submit report assessing the need and appropriateness of **extending the scope** of DORA to these entities
- COM to submit a legislative proposal (considering central bank oversight) in the **review of PSD2**, if appropriate

Financial markets infrastructures
→ cannot benefit from exemptions microenterprises

Statutory auditors and **audit firms**
→ report by COM 3 years after entry-into-force

Issuers/providers of crypto-assets → aligned with MICA

Ancillary insurance intermediaries
→ in scope (except for micro, small and medium entities)



DORA preliminary outcome for proportionality

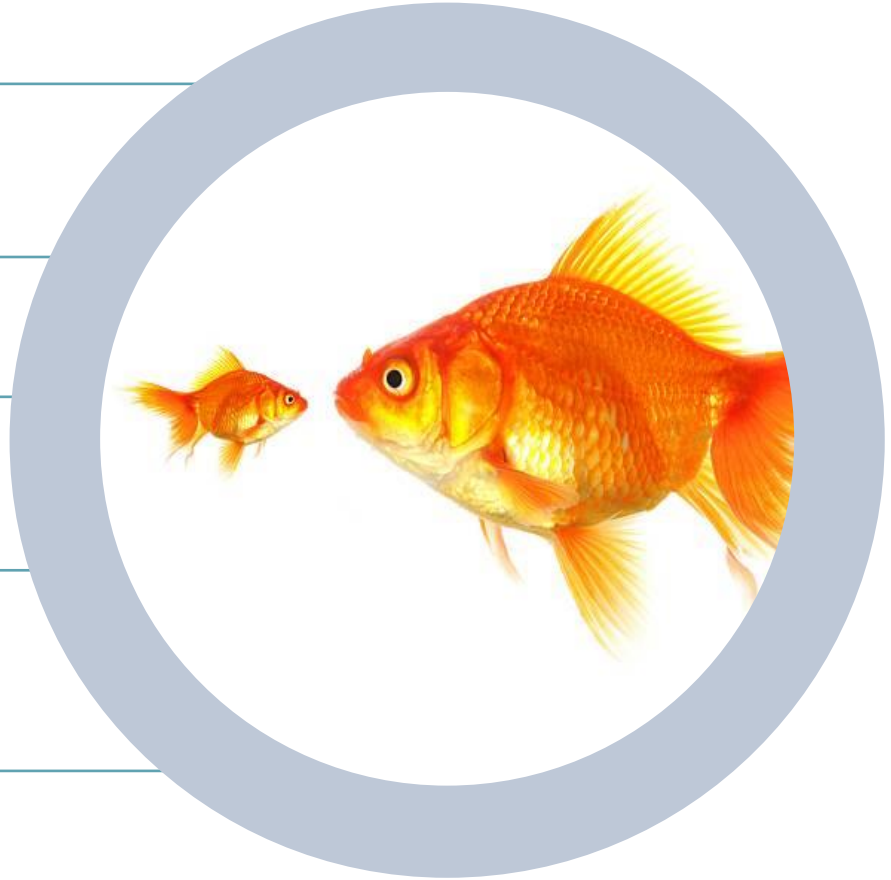
Proportionality principle **embedded throughout the text** (considering size, nature, scale and complexity of services, activities, operations, and overall risk profile)

Exemptions → in line with sectoral Union legislation

Microenterprises → much lighter regime (governance and risk management, testing, …)

Simplified ICT risk management framework
→ in function of size and services provided

Critical or important functions
- Some provisions specifically target "critical or important functions"



DORA preliminary outcome for incident/threat reporting

PSD2 major incident notification **fully integrated**

Time limits to be set at level 2, but ESAs' mandate will require consistency with **NIS2** (or to duly motivate any deviation)

ECB significant institutions
→ via NCA (immediate forward to ECB)

To public non-financial authorities
→ MSs can choose: 1) via NCA, 2) directly by FI

EU incident reporting hub
→ feasibility study report **24 months** after entry-into-force

Reporting of significant cyber threats
→ voluntary (aligned with NIS2)

DORA preliminary outcome for advanced resilience testing (TLPT)

RTS should be «**in accordance with TIBER-EU**»

Live production systems

- **Internal testers** allowed under **conditions**
  - External testers mandatory every 3rd test
  - Independence, capacity, no conflict of interest …
  - After approval by NCA
- … but not allowed for SSM SIs
- **Threat intelligence** always external

- MS can **designate** single public authority responsible for TLPT at national level
- Otherwise, a competent authority may **delegate** some/all tasks to another national authority

- Threat led penetration test (TLPT) at least **every 3 years**
- Some **flexibility** for NCAs on a case-by-case basis

Possibility for **pooled TLPT** for ICT TPP providing (same) service(s) to several financial entities

DORA preliminary outcome governance oversight framework critical TPPs

Structure
- **Oversight Forum** → subcommittee of the ESAs' Joint Committee
- **Lead Overseer** → one of ESAs (dependent FIs' assets)
- **Joint Oversight Network** → operational coordination
- **Joint Examination Team** → investigations/inspections

Designation criteria
- **Intra-group** providers not to be designated (criteria to be further specified by COM)
- **# MSs** in which service is provided/used no longer a criterion, but no designation if only provided in one MS

Subsidiary in EU within 12 months following designation

Follow-up reco's: LO may issue recommendations to CAs to promote consistent and convergent supervisory follow-up

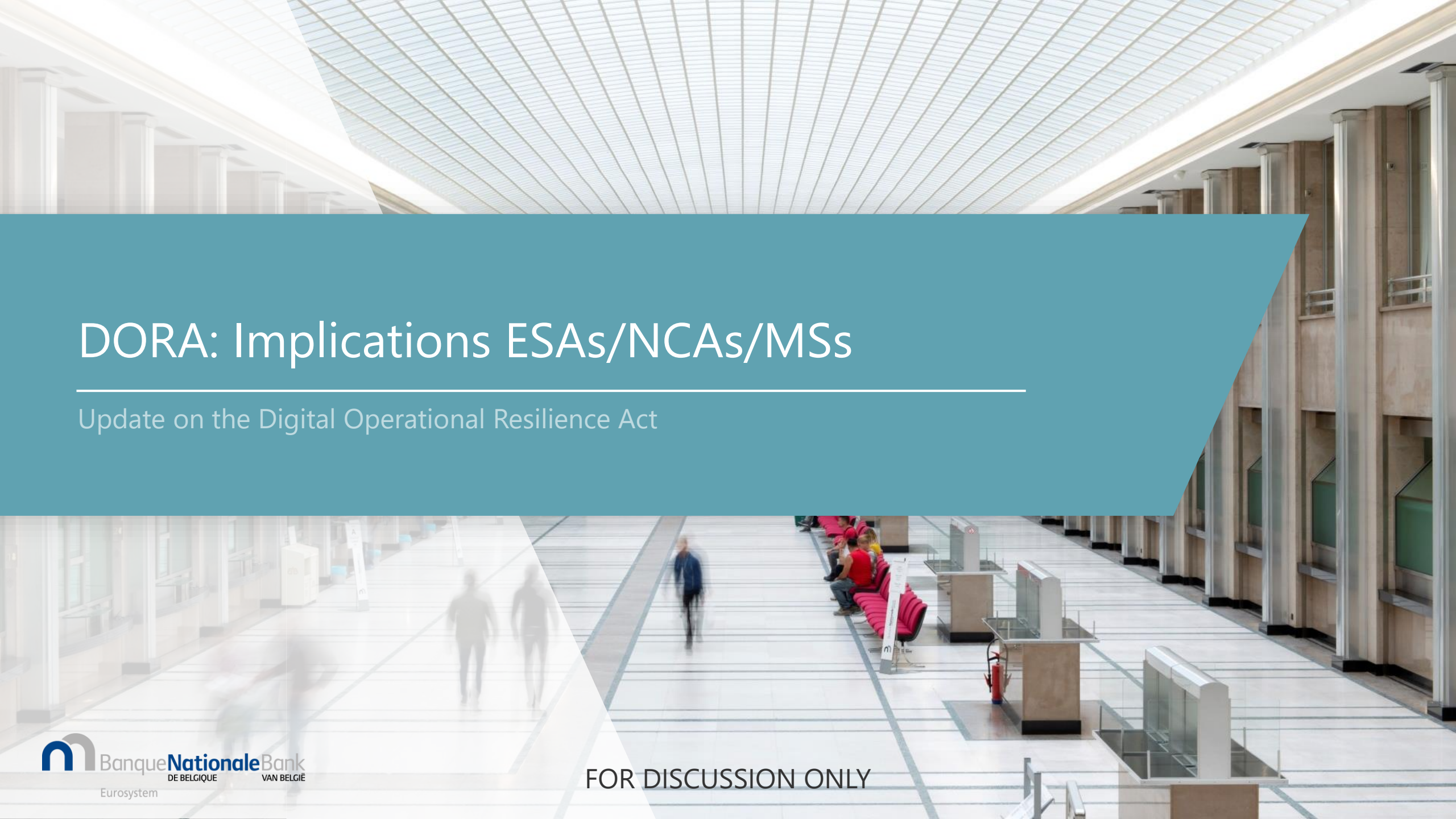
Oversight fee-funded, but preparatory development of **IT systems** via **NCA** contributions and **Union funding**

DORA preliminary outcome - other aspects

Third-party risk management
- **Multi-vendor** strategy → fully optional
- **Intra-group** TPP dependencies → not less risky

Timing
- **Application** → 24 months after entry-into-force for the whole text
- **Level 2 mandates** → 12-18-24 months

National security → without prejudice to the responsibility of Member States regarding essential state functions concerning public security, defence and national security



DORA: Implications ESAs/NCAs/MSs

Update on the Digital Operational Resilience Act

Banque Nationale de Belgique / Bank van België
Eurosystem

FOR DISCUSSION ONLY

ESAs' deliverables/implementation plan for DORA

EBA EUROPEAN BANKING AUTHORITY

esma European Securities and Markets Authority

eiopa European Insurance and Occupational Pensions Authority

Joint-ESAs policy mandates

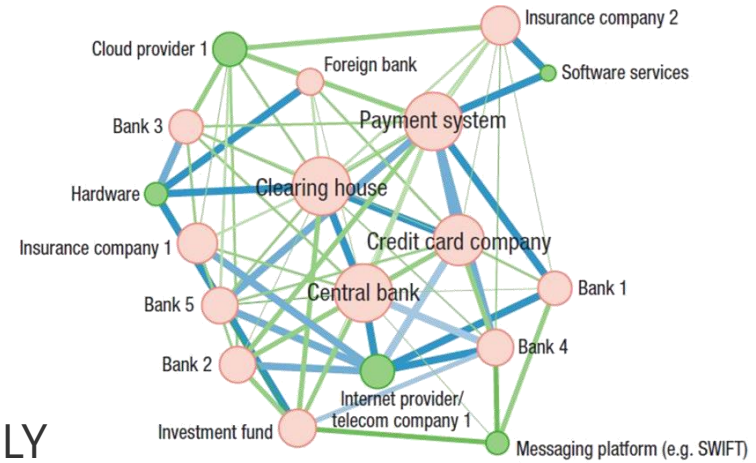
New JC sub-committee on Digital Operational Resilience:

- RTS, ITS, guidelines, feasibility report within 24 months (see annex)
- ESRB recommendation on pan-European systemic cyber incident coordination framework
- Cross-sectoral coordination, exchange of information, …

Start-up EU oversight activities

Joint ESAs exercise on collection of ICT 3rd party arrangement registers

- Improve understanding of use ICT third party providers across the EU financial sector
- Sample of financial entities
- Launched 19/7/'22
- Deadline 28/10/'22



NCAs: new DORA-related NCA activities/responsibilities

Contribution to **ESA policy mandates**

(see previous slides)

Notifications of **major incidents** (and significant **cyber threats**)

- **collection** (for the entire DORA scope)
- **acknowledge receipt** and (where feasible) provide relevant and proportionate **feedback** or high-level **guidance**
- review/assess **crisis communication** and management **actions/implemented changes**, estimations of aggregated annual **costs/losses**
- further **transmission** (+ evaluation **criteria**) (e.g. ESA, ECB, NIS authorities, resolution authorities, other relevant public national authorities (e.g. data protection authorities, law enforcement authorities), other competent authorities (in other MSs), …)

Oversight on **critical TPPs**

- representation in **Oversight Forum** and **joint examination teams**
- **inform** FIs of and **verify** their **compliance** with oversight **recommendations**, **require** and **assess** additional **measures** (e.g. suspension/ termination contracts), …
- collection and transmission to ESAs of **registers with 3rd party arrangements**

Threat-Led Penetration Testing (NCA or another national authority in the financial sector)

- **identify FIs** required to perform TLPT
- reduce/extend TLPT **frequency** (standard = every 3 years)
- **validate** the precise **scope** of tests as determined by FIs
- approve the use of **internal testers** (based on criteria)
- review of **attestation**, **summary** of the relevant **findings** and **remediation plans**

Reviewing/assessing

- the consistency/completeness of the **ICT risk management framework** (taking into account proportionality principle)
- results of the ICT **business continuity tests** or **similar exercises**
- ICT **third party arrangements**
- participation in the **information-sharing** arrangements
- …

Other

- foster **coordinated approach** with **NIS authorities** (e.g. participation in work of Cooperation Group)
- publish **administrative penalties**
- …

Actions member states

Member States shall:

- designate **single** NCA as **addressee** for reporting of **incident/threat notifications** (if FI supervised by > 1)
- designate the NCA whose staff member shall be the **high-level representative** in the **Oversight Forum**
- lay down rules establishing appropriate **administrative penalties and remedial measures** and **confer** on **CAs** all the necessary **powers**
- …

Member States may:

- determine that (some) FIs shall also provide **major incident notifications** (**directly**) **to NIS authorities**
- designate a **single public authority** as responsible in the financial sector, at national level, for all **threat led penetration testing** matters
- **exempt FIs** where this is possible according to DORA (and inform the EC)
- …

Interplay CER & NIS2

NIS2

- Horizontal Directive on measures for a high common level of **cybersecurity** across the Union
- Scope: a.o. **credit institutions**, **operators of trading venues**, **central counterparties** (size-cap rule)
- **DORA constitutes a 'lex specialis'** to NIS2 for the financial sector…
- but FEs designated under NIS2 remain part of the **'NIS ecosystem'** (e.g. national strategies, information exchange with CSIRTs, representation in Cooperation Group, etc.)
- **Minimum harmonisation**: MS can in principle extend the **scope** or adopt **more demanding provisions**

CER

- Horizontal Directive on the resilience of critical entities (**physical security**)
- Scope: a.o. **credit institutions, operators of trading venues, central counterparties** designated as critical entities (=> essential under NIS2)
- **NIS2 'lex specialis'** in relation with CER**?**
- **Minimum harmonisation**: MS can in principle extend the **scope** or adopt **more demanding provisions**

Interplay CER & NIS2 (for entities in scope of DORA)

DORA

Cyber risk (incl. physical security of ICT infrastructure) of financial entities

?

Cyber risk (incl. physical security of ICT infrastructure) of essential or important entities within highly critical or critical sectors

CER

except art. 11 and chapters III, IV and VI

NIS2

except chapters IV and VII

Physical security of critical entities

DORA: Impact financial entities

Update on the Digital Operational Resilience Act

Banque Nationale de Belgique / Bank van België
Eurosystem

FOR DISCUSSION ONLY

Impact financial entities

Depends largely on:

- The **size** of and **services provided** by your entity,
- Whether your entity was already the subject of **specific sectoral guidelines/expectations:**
  - **EBA:**
    - Guidelines on ICT and security risk management (EBA/GL/2019/04)
    - Guidelines on outsourcing arrangements (EBA/GL/2019/02)
    - Revised Guidelines on major incident reporting under PSD2 (EBA/GL/2021/03)
  - **EIOPA:**
    - Guidelines on ICT security and governance (EIOPA-BoS-20/600)
    - Guidelines on outsourcing to cloud service providers (EIOPA-BoS-20-002)
  - **ESMA:**
    - Guidelines on outsourcing to cloud service providers (link)
  - **ECB:**
    - Cyber resilience oversight expectations for FMIs (link)
- And of course, **your compliance** with this already existing regulatory guidance…

How to prepare?

No-regret actions:

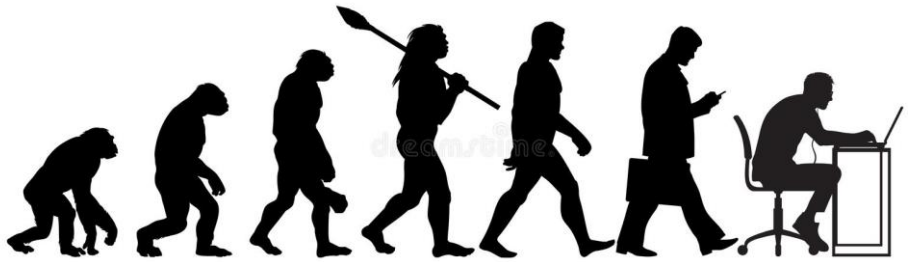
- Create **internal awareness** on DORA scope & process
- Follow-up on **level 2 texts** (RTS and ITS) + **choices member states**
- **Review** the policies/processes/capabilities for **gaps** w.r.t.:
  - **ICT risk management** governance, organization and framework
  - Detecting/managing/classifying **ICT-related incidents/threats** (assessing impact/root cause, communication plans, etc.)
  - **Resilience testing** programmes (risk-based, adequate coverage, independent, remediation assured)
  - **Third-party risk management** (strategy, policies, assessment practices, exit plans, contractual terms)
    - Create an **inventory** of all **ICT third party arrangements** (incl. material **sub-contracting**) -> format ESAs' exercise is indicative, but will still change (ITS)
  - **Information & intelligence sharing** (confidentiality, data protection, etc.)
- Start **developing roadmaps** and make provisions in **budgetary planning**

Generic NBB observations from the past

- **Controls** can still be improved in many areas. Special attention seems warranted for:
  - **Building (and maintaining) core IT competencies** (also at board level),
  - **IT risk management framework** (roles & responsibilities, risk treatment & monitoring),
  - **# audits** and **remediation** of critical audit findings,
  - **Stocktaking** and **classification** of **IT assets** (incl. data) and **configuration management**,
  - **Alignment with IT security best practices** (monitoring and detection capabilities, prevention of data loss, system hardening, End-of-Life systems, privileged access, segregation of duties, SDLC, …),
  - Management and monitoring of **ICT third-party risks** (risk assessments, mitigating measures, contract clauses, reporting by service provider, exit plans, …),
  - **Representative** IT **continuity/security testing** (extreme but plausible scenarios),
  - Management of **End-User-Computing** applications,
  - …

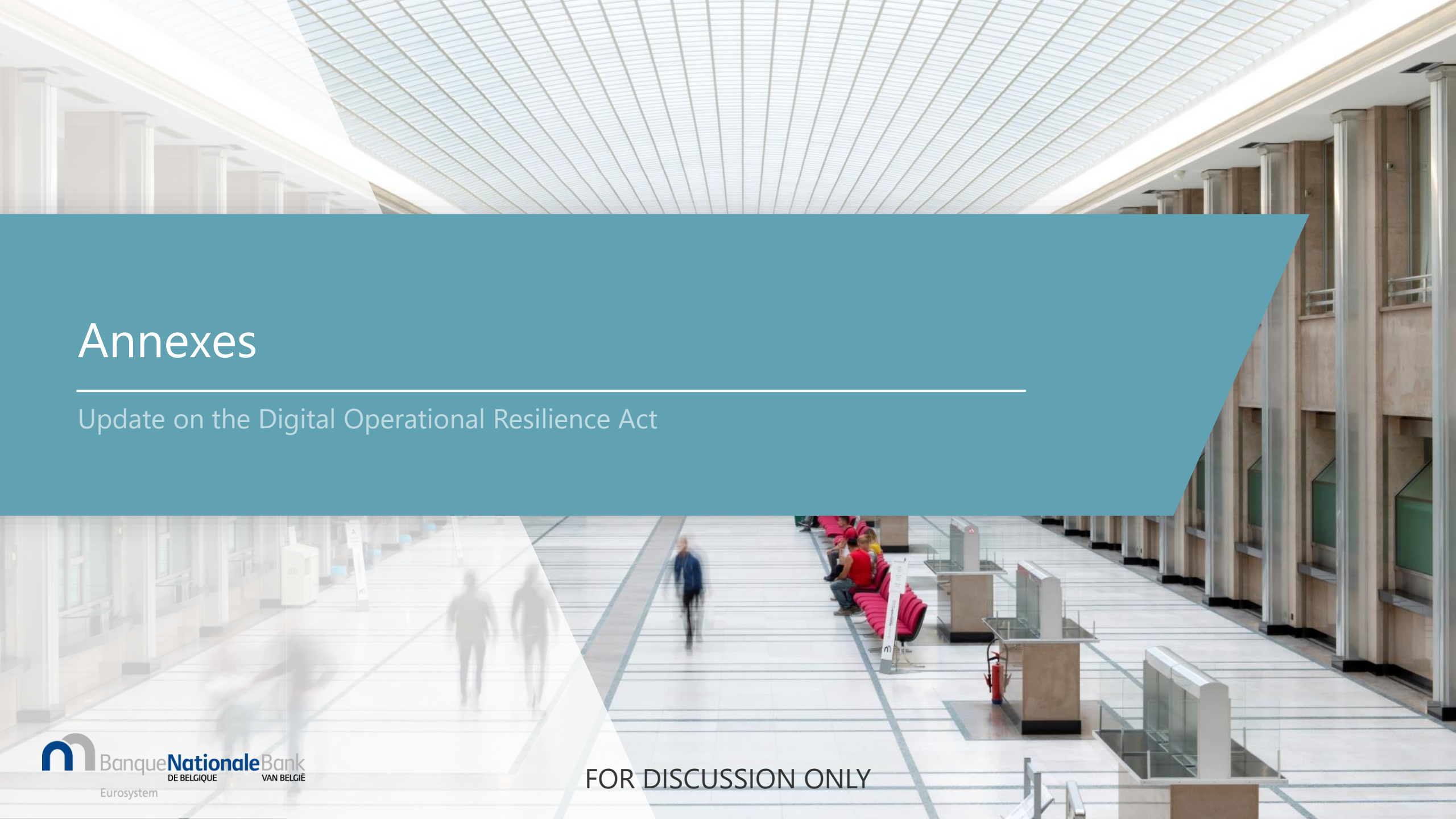
Already existing supervisory expectations?

- Existing **supervisory policy documents** (ESA guidelines, NBB circulars) **to be revised**,
- But **expectations beyond DORA** are presumably there to stay:
  - ESAs to **identify the overlap** between their guidelines and DORA and **adapt** the former **accordingly**?
  - NBB to **update** but **not** to **withdraw** the expectations that address very **specific risks** or a very **specific scope**. Examples:
    - Circular NBB_2015_32 - Additional prudential expectations regarding operational business continuity and security of systemically important financial institutions
    - Circular CBFA_2009_17 - Financial services via the Internet: Prudential requirements (incl. annex)



Off-line questions:

- NIS2: orm@nbb.be
- Swift oversight: Permsec.Swift_oversight@nbb.be
- TIBER-BE/TLPT: tiber-be@nbb.be
- DORA in general/NBB policy framework for IT/cyber risk: it.supervision@nbb.be



Annexes

Update on the Digital Operational Resilience Act

Banque Nationale de Belgique / Bank van België
Eurosystem

FOR DISCUSSION ONLY

Annex 1: Glossary

- CTPPs, TPSPs, SPs….: (critical) 3rd-party (service) provider(s)
- COM, EC: European Commission
- DG-FISMA: The Directorate-General for Financial Stability, Financial Services and Capital Markets Union is the Commission department responsible for EU policy on banking and finance
- DLT: Digital Ledger Technology
- ESA: European Supervisory Authorities
  - EBA: European Banking Authority
  - EIOPA: European Insurance and Occupational Pensions Authority
  - ESMA: European Securities and Markets Authority
- FI: Financial institution
- GL: Guidelines
- LO: Lead Overseer
- MS: Member state
- NIS/NIS2: (Revised directive on Security of)Network and Information Systems (v2 – proposed by EC 2020)
- PI/ELMI: Payment institution / Electronic money institution PSD2: Payment Service Providers Directive (v2 – proposed by EC 2013, entry into force in 2018)
- RTS/ITS: Regulatory & Implementation Technical Standards (“level 2”)
- TLPT: Threat led penetration testing

Annex 2: Other EU legislative initiatives + interplay with DORA

NIS(2)	• **Horizontal** Directive **on measures for a high common level of cybersecurity** • **DORA** constitutes a '**lex specialis'** to NIS2 for the financial sector • **FEs** designated under NIS2 Directive **remain part of** the **'NIS ecosystem'** (e.g. national strategies, information exchange with CSIRTs, representation in Cooperation Group, etc.)
CER	• **Horizontal** Directive on the **resilience** of **critical entities** • **Physical security** • **Specific obligations** (chapters III and IV) **do not apply** to FEs (under DORA)
PSD2 (PSD3?)	• **Payment Services** Directive • **Notification** of **major incidents integrated** in DORA • COM to submit, if appropriate, a legislative proposal on **payment systems/processing activities** (considering central bank oversight)
Cybersecurity and **Cyber resilience Acts**	• **Strengthens** the EU Agency for cybersecurity (**ENISA**) and establishes a cybersecurity **certification framework** for **products** and **services** • Mandatory **cybersecurity requirements** for **products with digital elements**, throughout their **whole lifecycle**
Information Security and **Cybersecurity Regulations**	• Uniform **information** (classification and protection) and **cybersecurity** (~NIS2) **rules**, applicable to **EU institutions**, **bodies** and **agencies**

Annex 3: DORA chapters … details (1)

Ch II: ICT Risk Management

- Governance and organisation, ICT risk management framework
- ICT systems, protocols and tools (maintain, fit for purpose, reliable, capacity)
- Identification, Protection and Prevention, Detection, Response and recovery
- Backup policies and recovery methods
- Learning and evolving, Communication
- Further harmonisation of ICT risk management tools, processes and policies

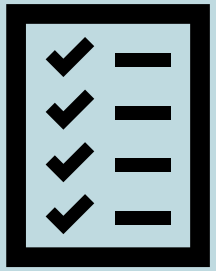
Ch III: ICT-related incidents

- ICT-related incident management process
- Classification of ICT-related incidents
- Reporting of major ICT-related incidents
- Harmonisation of reporting content and templates
- Centralisation of reporting of major ICT-related incidents
- Supervisory feedback

Annex 3: DORA chapters … details (2)

Ch IV: Digital operational resilience testing

- Testing of ICT tools and systems (“Basic testing”)
- Advanced testing of ICT tools, systems and processes based on TLPT (“Threat Led Penetration Testing”)



Ch V: Managing of ICT third-party risk

- Key principles for a sound management of ICT third party risk
  - Preliminary assessment of ICT concentration risk and further sub-contracting
  - Key contractual provisions
- Oversight framework of critical ICT third-party service providers
  - (See next slide)

Annex 3: DORA oversight framework for CTPP's

Request for information, General investigations, On-site inspections, Ongoing Oversight

Harmonisation of conditions enabling the conduct of the Oversight

Follow-up by competent authorities, Oversight fees, International cooperation

Designation of critical ICT third-party service providers

Structure of the Oversight Framework, Tasks of the Lead Overseer, Oversight Powers

Oversight framework of critical ICT third-party service providers

Annex 4: DORA joint-ESAs policy mandates

	Policy mandate	Delivery (after entry into force)		
		12 months	18 months	24 months
1	RTS on ICT risk management framework (art. 14)	X		
2	RTS on simplified ICT risk management framework (art. 14a.3)	X		
3	RTS on criteria for the classification of ICT-related incidents (art. 16.2)	X		
4	Guidelines on the estimation of costs/losses caused by major ICT-related incidents (art. 10.9a)		X	
5	RTS on specifying the reporting of major ICT-related incidents (art. 18.1a)		X	
6	ITS to establish the reporting details for major ICT-related incidents (art. 18.1b)		X	
7	Feasibility report on single EU Hub for major ICT-related events (art. 19.1)			X
8	RTS to specify threat led penetration testing aspects (art. 23.4)		X	
9	ITS to establish the templates for the Register of information (art. 25.10)	X		
10	RTS to specify the policy on ICT services (art. 25.11)		X	
11	RTS to specify elements when sub-contracting critical or important functions (art. 27.4)		X	
12	GL on cooperation between ESAs and CAs regarding the structure of the oversight (art. 29.4)		X	
13	RTS to specify information on oversight conduct (art. 36.1)		X	