Orange
Cyberdefense
Ahead of the Storm

The European Digital Operational Resilience Act (DORA)

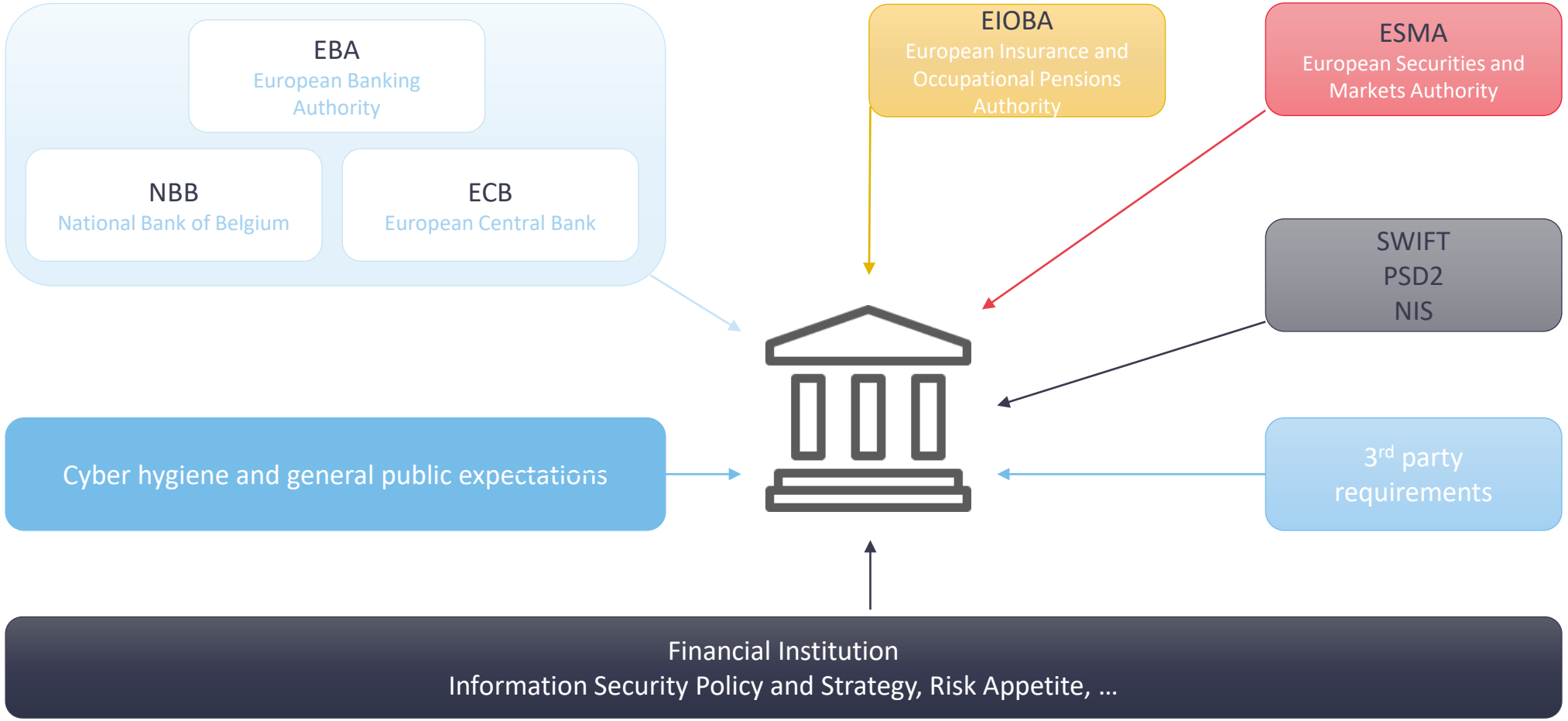
Karine Goris, Chair of the Security Advisory Board at Febelfin

Dan Cimpean, Director Risk Advisory at BDO

febelfin BDO Belfius orange

Current sectoral expectations vs DORA

Many regulatory requirements are already in place today. DORA can be seen as an evolution of bringing together and advancing the requirements that already exist for (systemic) Belgian Banks. Proportionality and risk-based are principles that also apply.



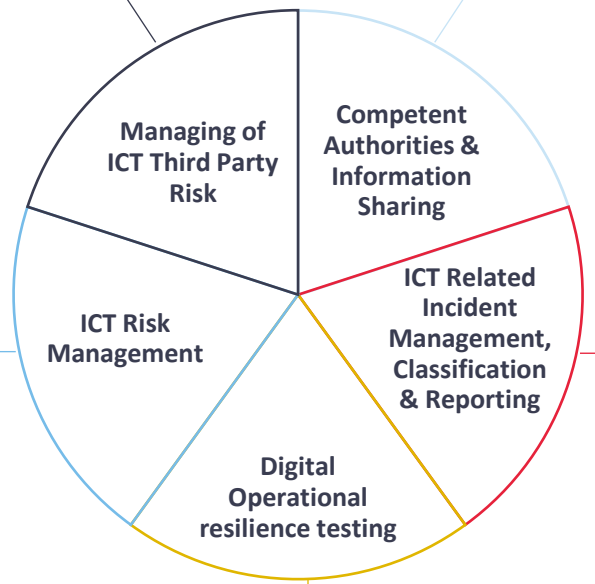
DORA – a view from a regulator perspective

- DORA to set the basis for digital resilience at financial entities
- Financial entities are required to improve their digital resilience
- Enhancing IT risk management processes, incident handling, management of third parties, sharing cyber-related information and experiences with peers
- DORA goes into effect 24 months after its official adoption

Overall challenges

Financial institutions are heavily interconnected with, or dependant on, 3rd parties. The big challenge is to remain in control.

Information sharing is key and encouraged between the Belgian banks. Sharing information on the European level could be beneficial, but financial institutions need to balance efforts versus benefits.



Prepare for compliance with the regulation, identify the GAPs and review processes, provision budgets and ensure that you have the evidences to support your compliance in the future.

Collect the relevant ICT incident information in the correct templates and ensure that the process allows communication to the regulator in due notice.

Recovery was typically focussed on operational incidents / calamities. Resilience will require e.g. cyber threats to be added in the mix.

State of play for financial entities in EU & BE

- Certain sectors are being subject to such regulations for the first time (crowdfunding organizations, credit rating agencies, benchmark administrators)
- They lack IT, risk and cyber frameworks and have limited experience in translating IT regulations into controls within their organizations
- Financial entities do not have yet good practices or controls in place through existing regulations that address information sharing agreements
- Credit institutions, insurers and pension funds - have experience in implementing IT regulatory requirements such as EBA Guidelines on ICT & Security Risk Management, EBA Guidelines on Outsourcing or EIOPA ICT Guidelines still make efforts to comply with DORA in a pragmatic manner

View on - ICT Risk Management

1) Security and digital operational resilience competencies at all levels, including board.
2) Classification of assets / data and link to infrastructure.
3) Information Security Management System monitoring the link between the policies and environment and overall compliance with regulations.

View on – ICT-related incidents

Process & classification

Centralization

Reporting

1) Incident management process including the classification methodology.
2) Centralize (major) ICT-related incidents to ensure the regulator can be notified in due notice.
3) Reconcile incident reports and templates to ensure the required information is included.

View on - Digital operational resilience testing

Basic testing

Advanced testing

Threat Led Penetration Testing (TLPT)

1) Prepare for the unexpected and consider “when” instead of “if”. Advance DRP and cyber programs into an overall resilience program.
2) Threat Led Penetration Testing of ICT tools, systems and processes for significant financial entities is in place via TIBER-BE.
3) Include EU-based critical third-parties in the preparation of the TLPT exercise.

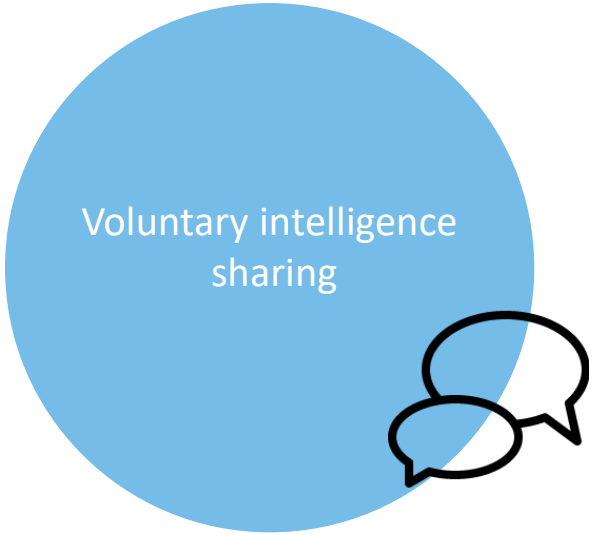
View on - Managing ICT 3rd party risk

1) Reconsider the business case for the cancelled Third Party Risk Management (TPRM) initiative between banks.

2) Contracts might need to be further reviewed compared to the EBA guideline scope (critical contracts) and revised where needed. ICT concentration risk to be evaluated for the cloud.

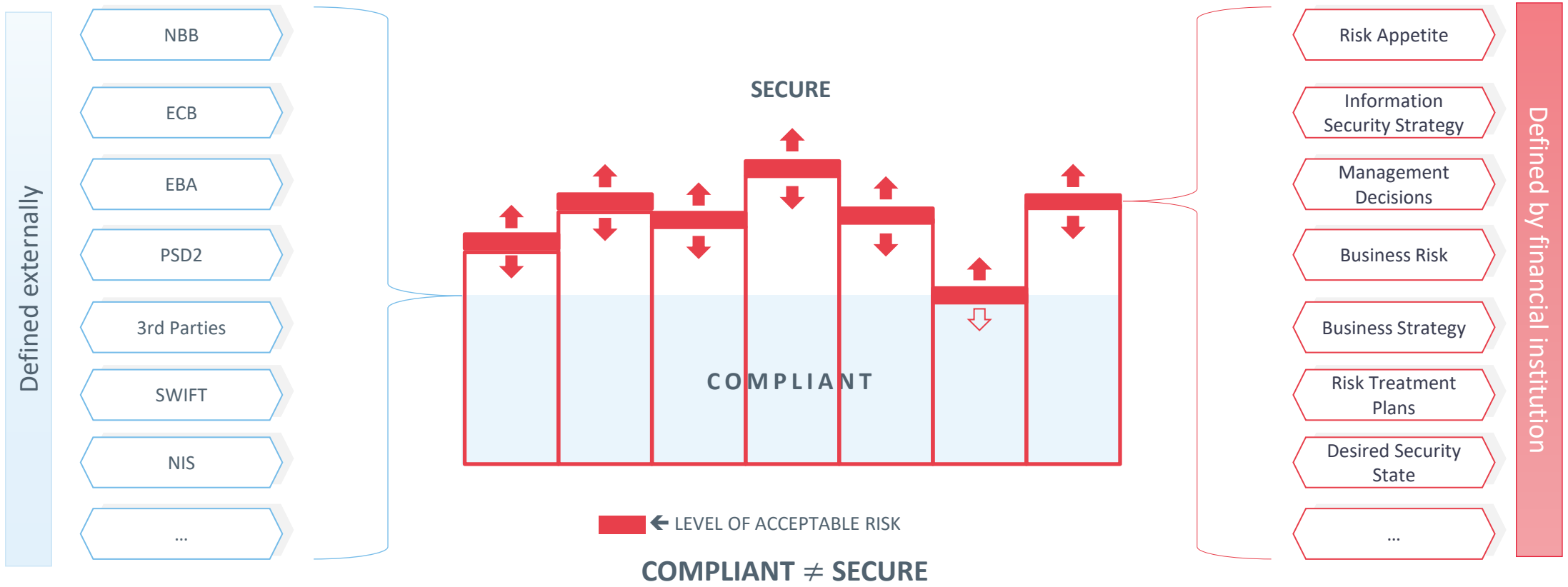
3) Bring together all information to correctly assess the risk posture of an ICT provider.

View on - Competent authorities & information sharing



1) In general this could be a layer on top of existing information sharing platforms used by the Belgian banks.
2) Finding balance between being informed on threat information, tactics, procedures and IOCs and being overwhelmed by it.
3) Maintain a view on what information can be shared to ensure no confidential / personal data is leaked.

You have to be compliant, you decide to be secure.



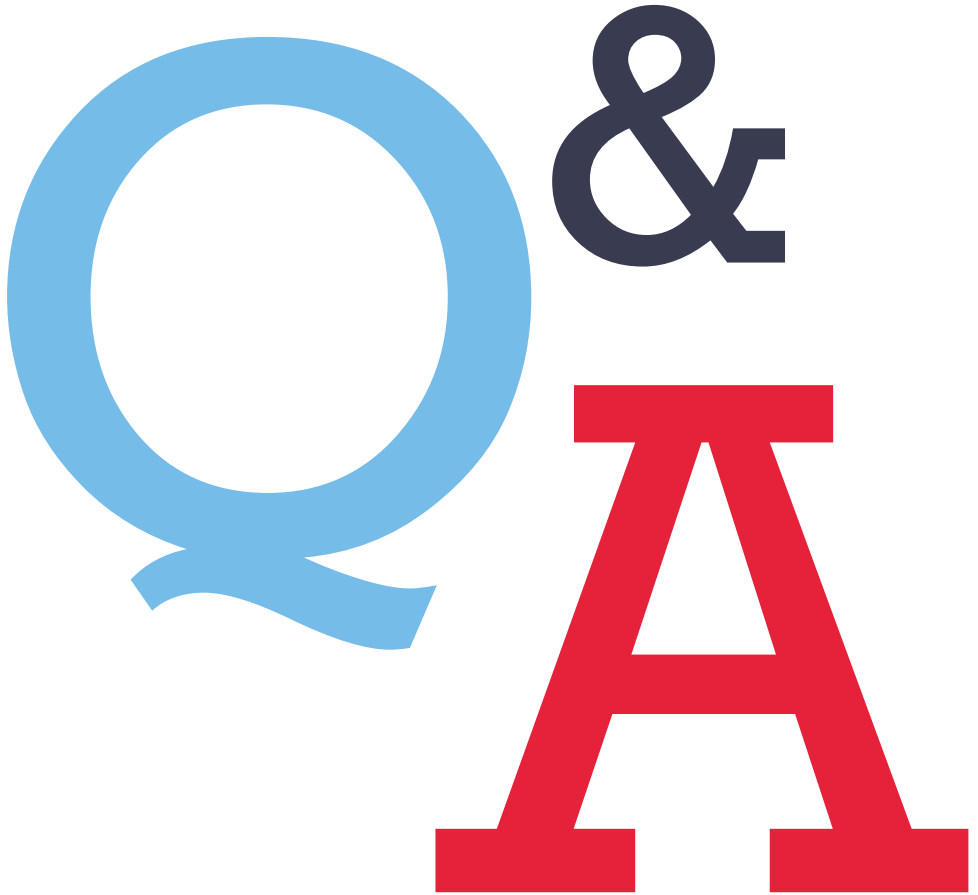
Engage with & keep an eye on regulators

- EBA's Work programme 2023 Vertical Priority VP#4 that focuses on digital finance and the delivery of MiCA/DORA mandates
- Implementing Technical Standards (ITS) on DORA incident reporting + ITS to establish the templates for the Register of information or specification of information security standards (DORA – Art25)

- Art. 37 grants the competence to NCAs to require a financial entity to terminate, in part or completely, the contractual arrangement with a Critical ICT Third Party Provider (CTPPs)
- Need for management of significant risk to the operational resilience and business continuity of the financial entity
- The reality of multiple innovative services being consumed by a financial entity under a shared contractual arrangement with a CTTP

Focus areas for financial entities

- ☑ DORA regulatory gap analysis and focus on what you need to remediate your gaps
- ☑ Educate, raise awareness and get buy-in from senior management
- ☑ Design ICT risk compliant management framework
- ☑ Digital operational resilience testing
- ☑ Design information sharing arrangements
- ☑ Budget for the DORA actions of the next 24 months



febelfin

Belgian Financial Sector Federation
www.febelfin.be