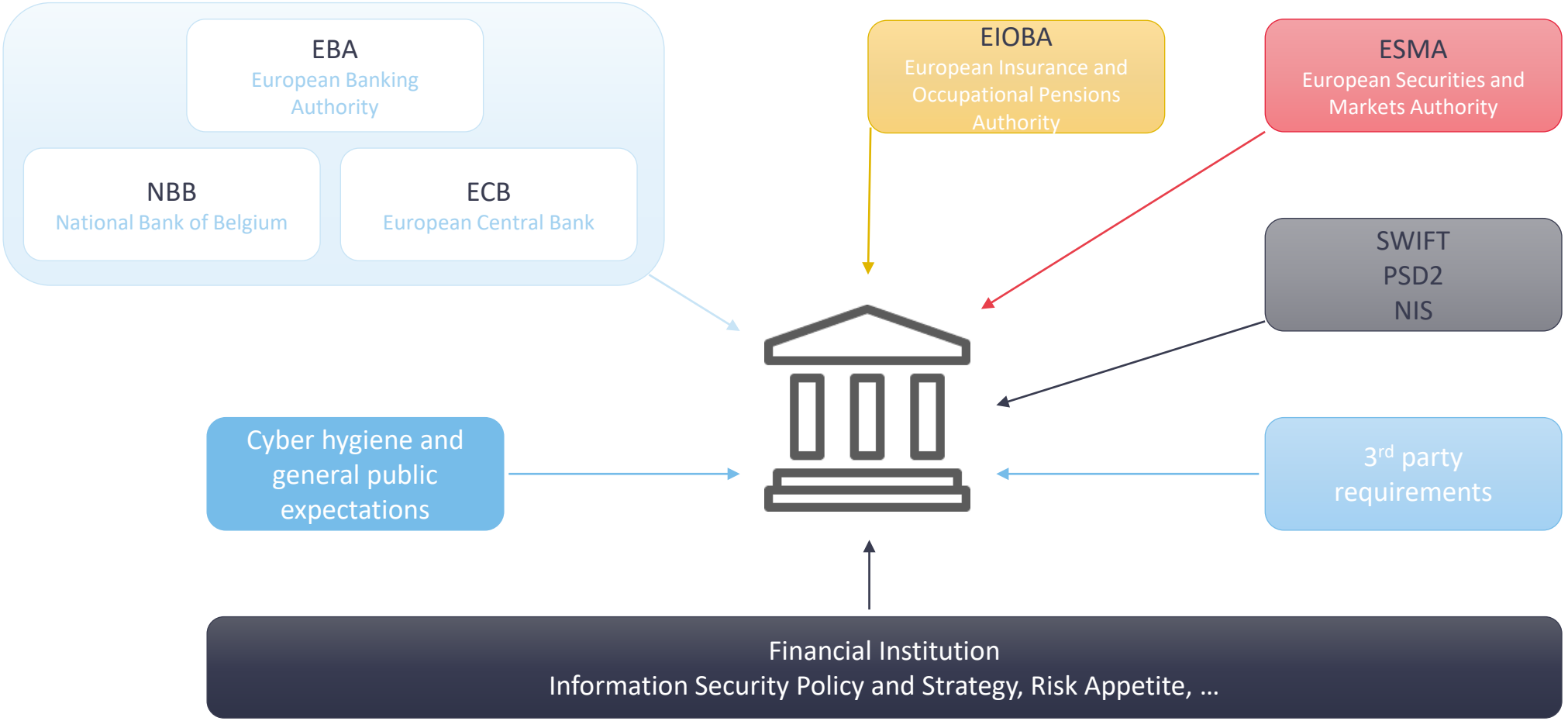
DORA

13/01/2023

Current sectoral expectations vs DORA

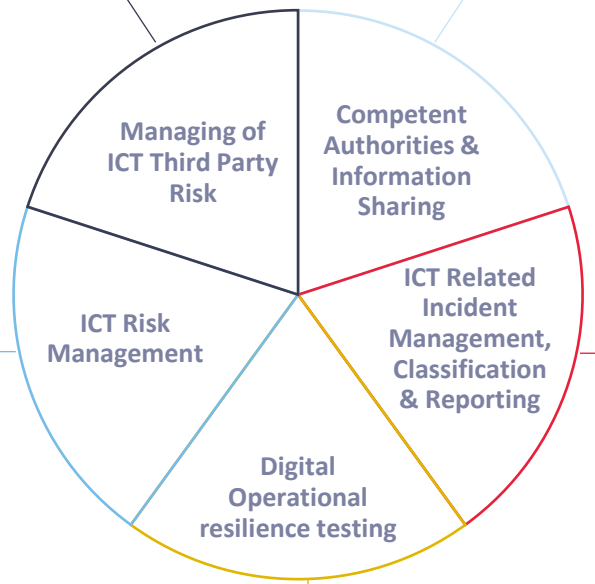
Many regulatory requirements are already in place today. DORA can be seen as an evolution of bringing together and advancing the requirements that already exist for (systemic) Belgian Banks. Proportionality and risk-based are principles that also apply.



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.

View on - ICT Risk Management

Governance, organization and policies

Identify, detect, protect, respond & recover

Learning & awareness

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

ICT 3rd part risk principles

Contractual provisions & register/framework

Due diligence & assessment

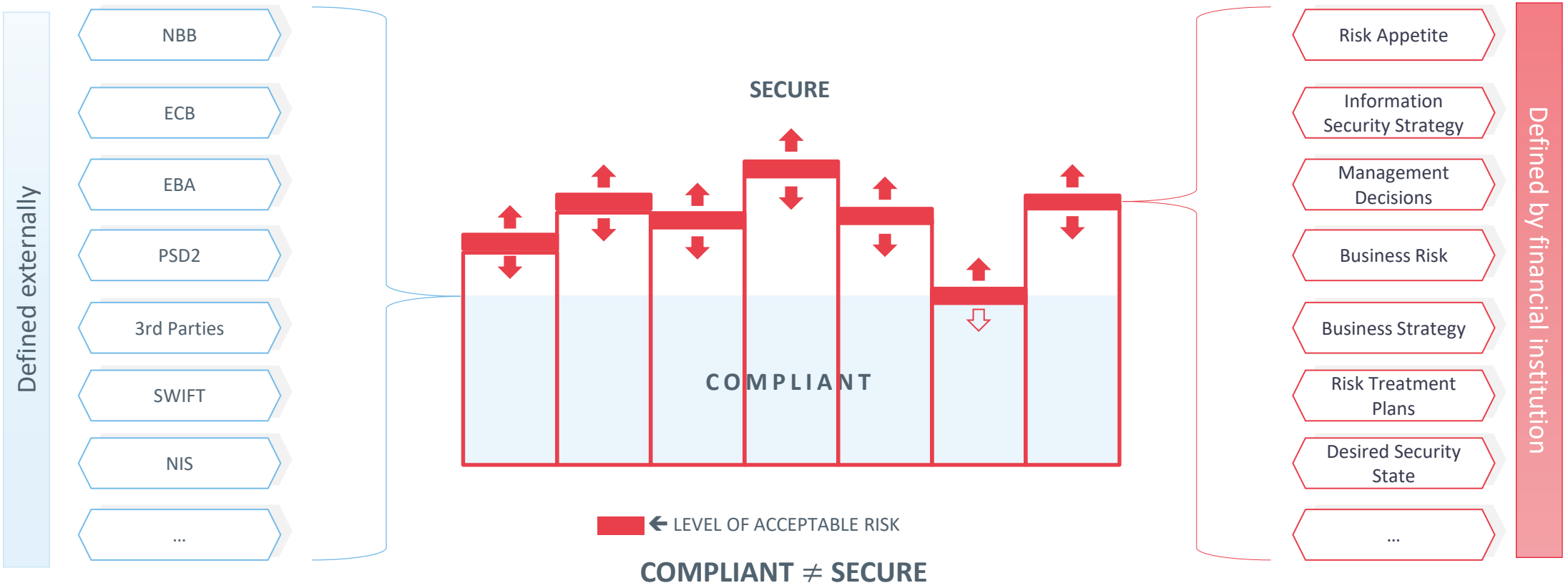
1) Reconsider the business case for the cancelled Third Party Risk Management (TPRM) initiative between banks.
2) Contracts might need to be further reviewed compared to the EBA guideline scope (critical contracts) and revised where needed. ICT concentration risk to be evaluated for the cloud.
3) Bring together all information to correctly assess the risk posture of an ICT provider.

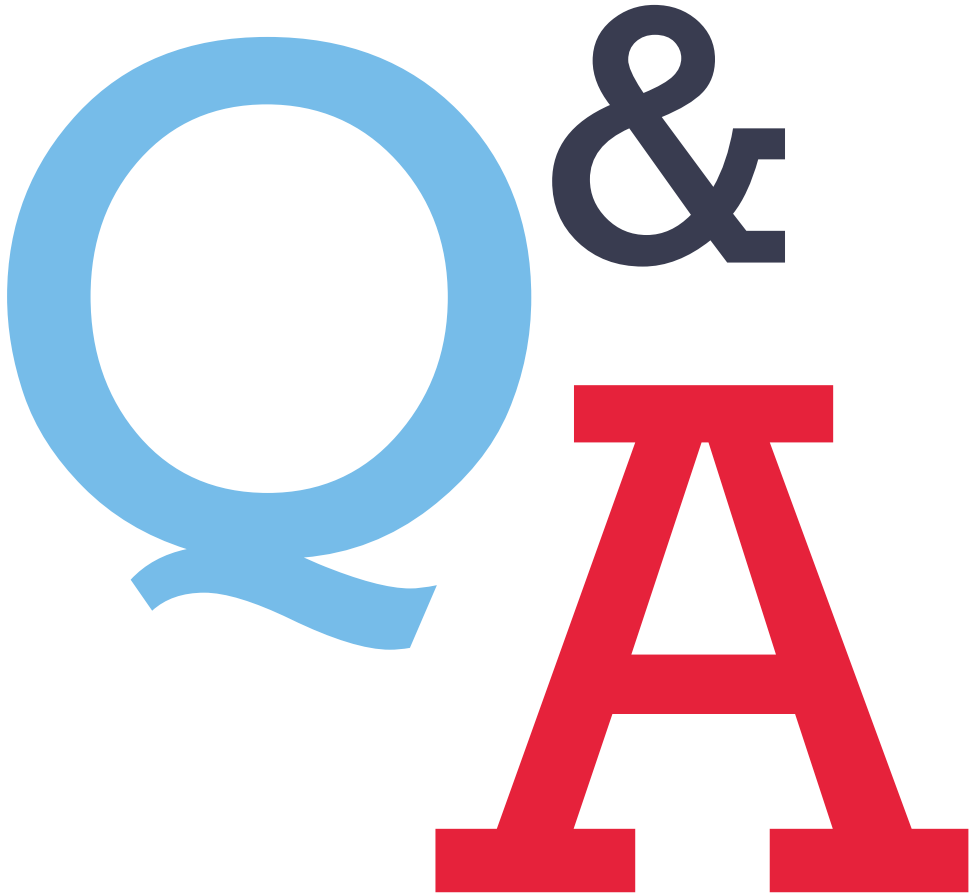
View on - Competent authorities & information sharing

Voluntary intelligence 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.




Q&A

febelfin

Belgian Financial Sector Federation
www.febelfin.be