National Bank OF BELGIUM
Eurosystem

EBA Guidelines on ICT and security risk management

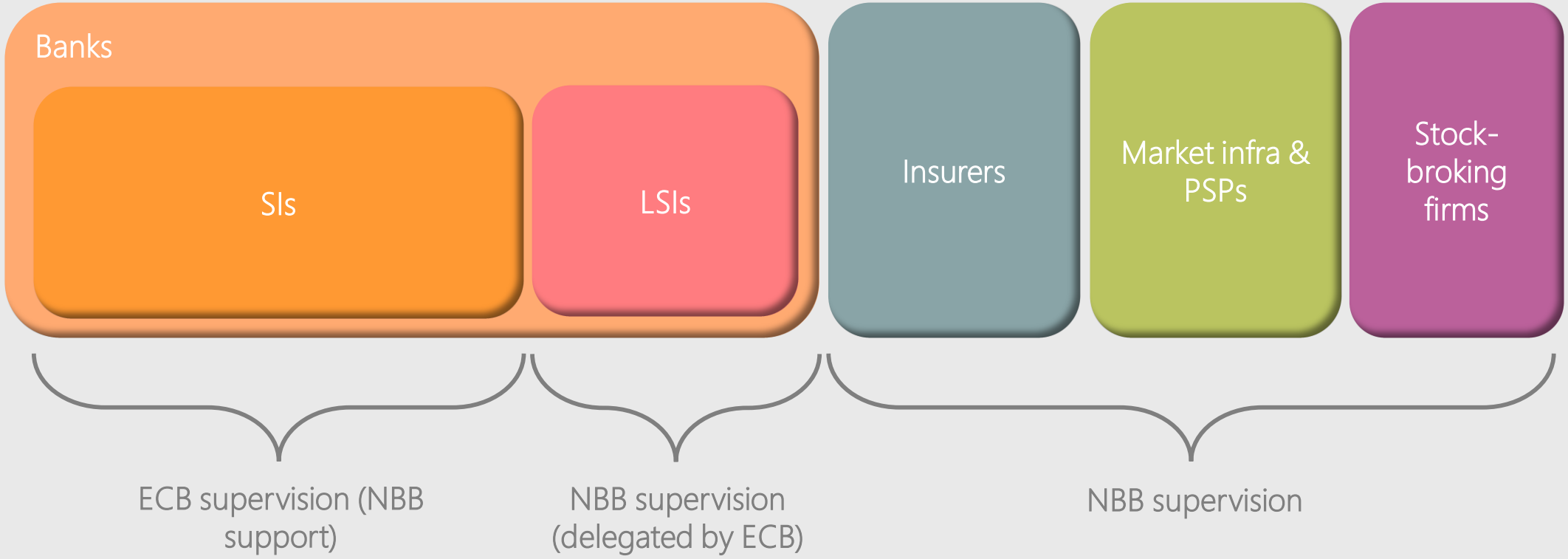
Thomas Plomteux, webinar Febelfin

26th of June 2020

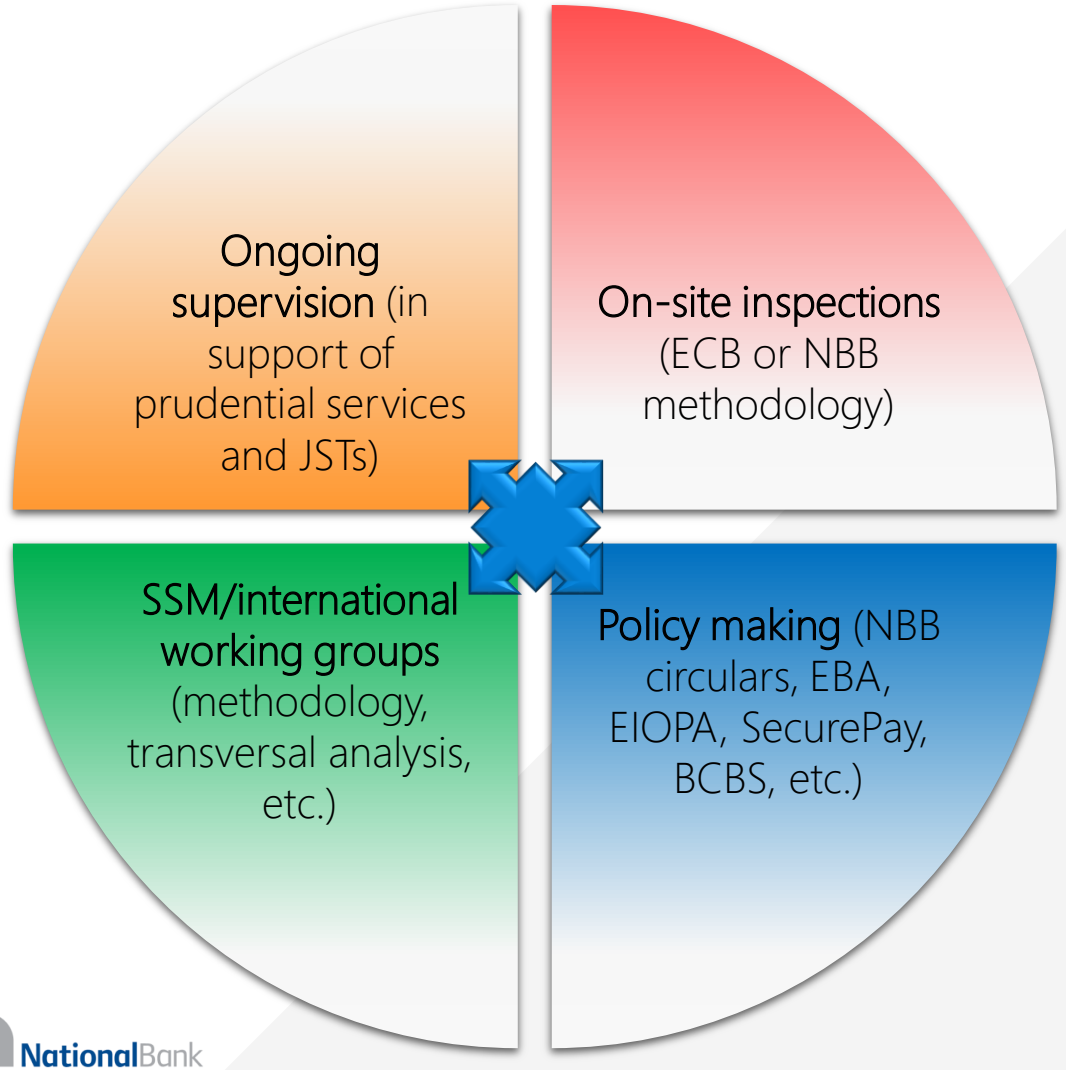
Overview

- IT prudential supervision NBB
- EBA Guidelines on ICT/cyber risk management
  - Integration in NBB policy framework
  - Content guidelines/public consultation
- Q&A

Scope prudential supervision NBB

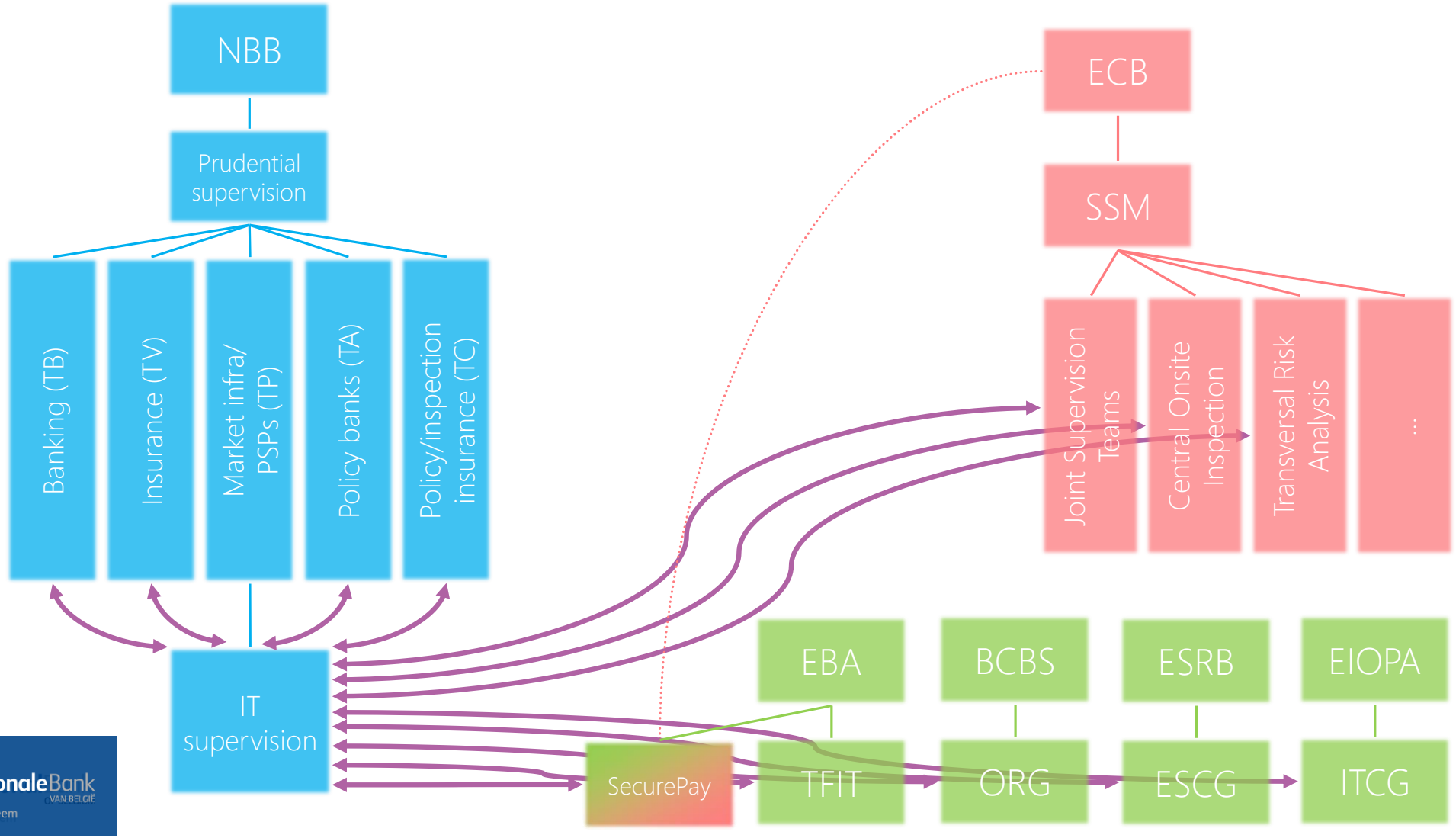


ITA introduction

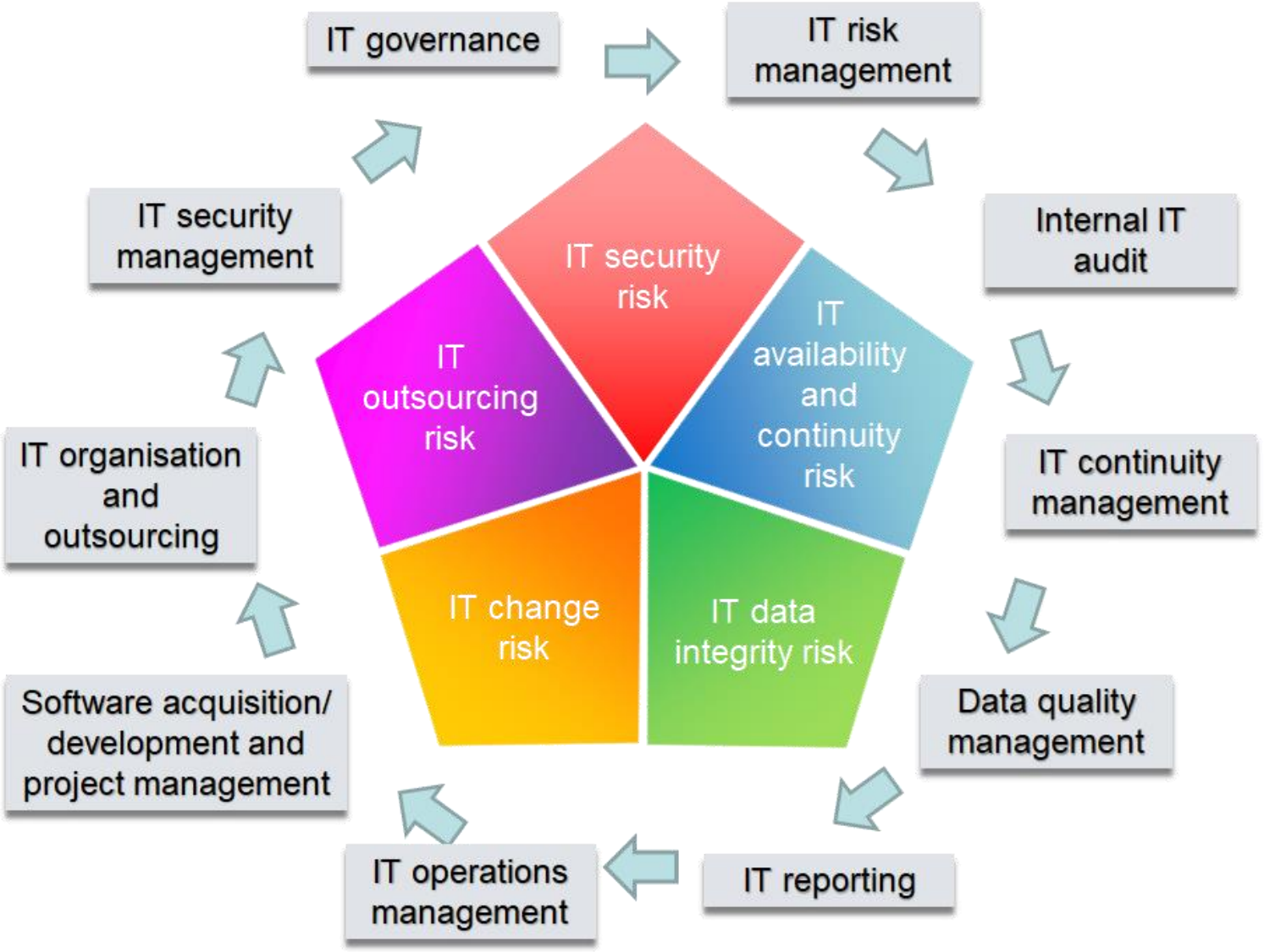


- IT expert centre
- Currently 8 FTE
- Supporting **all** prudential services
- Centralising IT expertise realizes **considerable economies of scale**:
  - Flexible risk-based allocation of resources
  - Knowledge sharing
  - Level playing field (within Belgium)
- Areas of expertise: **information security**, **IT continuity**, **IT outsourcing/cloud computing**, IT project risks, IT complexity, Fintech, data quality

Schematic overview interactions IT supervision NBB



IT/cyber risks and mitigating controls



Team

Thomas Plomteux

Yvanna Vieira de Melo Correa Mendes

Sarah Ben Aïssa

Rudi Pierquin

David Van Renterghem

Arthur Murzeau

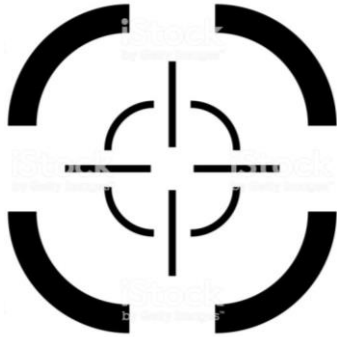
Dominique Bajusz

Gerardo De Guzman

Overview

- IT prudential supervision NBB
- EBA Guidelines on ICT/cyber risk management
  - Integration in NBB policy framework
  - Content guidelines/public consultation
- Q&A

Scope circular NBB_2020_23



- **Credit institutions** and **stockbroking firms** governed by Belgian law;
- **branches** established in Belgium of **credit institutions** and **stockbroking firms** governed by the law of a **non-EEA Member State**;
- **payment institutions** and **electronic money institutions** governed by Belgian law;
- **branches** established in Belgium of **payment institutions** and **electronic money institutions** governed by the law of a **non-EEA Member State***;
- in the context of consolidated supervision, group supervision or supplementary conglomerate supervision, **financial holding companies** and **mixed financial holding companies**.

* Assuming that the legal provision of which the content is specified in the circular is made applicable to the branches concerned.

Legal basis circular NBB_2020_23

- **Banking Law** of 25 April 2014 (**credit institutions** and **stockbroking firms**)
  - Article **21** -> Obligation to have a **sound and appropriate arrangement for the organisation of the business***
  - Article **168** -> **Financial holding companies** and **mixed financial holding companies** governed by Belgian law are also expected to comply on a **consolidated basis**
- **Payment Services Law** of 11 March 2018 (**payment service providers**)
  - Articles **21** and **176** -> Obligation to have **a sound and appropriate arrangement for the organisation of the business***
  - Articles **50-53** and **145** -> Establish a security policy as well as **procedures for reporting incidents**

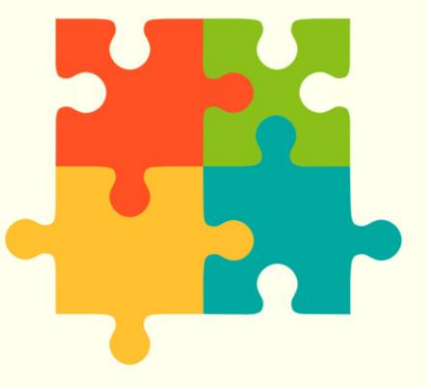
* These articles mention: an appropriate **management structure**, including a clear, transparent and coherent arrangement for allocating **responsibilities**; effective **procedures** for the **identification**, **measurement**, **management**, **monitoring** and internal **reporting** of the financial institution's **risks**; an appropriate **independent risk management function** and **internal audit function**; appropriate IT **control and security measures**; the introduction of appropriate **measures for business continuity**

Other clarifications circular NBB_2020_23

- EBA Guidelines on ICT and security risk management (EBA/GL/2019/04) **integrated in NBB policy framework** as of **June 30th 2020**
- "Guidelines on security measures for operational and security risks of payment services" (EBA/GL/2017/17) **integrated**. Therefore, this new circular **replaces NBB_2018_13**.
- **"Financial institutions"** in EBA Guidelines and circular refers to:
  - **payment service providers** (payment institutions, electronic money institutions and credit institutions) with respect to the provision of payment services;
  - **credit institutions** with respect to any of their activities other than payment services;
  - **investment firms*** with respect to any of their activities.
- Some **provisions** and **clarifications** aimed exclusively at payment service providers, credit institutions or "investment firms".

* For the scope of this circular, "investment firms" should be read as **"stockbroking firms"**.

Other IT/security related circulars



The EBA Guidelines should be read and applied in conjunction with the provisions of the following Circulars:

- NBB_2019_19 -> general expectations regarding **outsourcing** for this scope
- NBB_2015_32 -> specifically for **systemically important financial institutions**
- CBFA_2009_17 -> additional provisions for offering **financial services** (excluding payment services) **via the Internet** (inter alia for credit institutions and stockbroking firms)
- PPB 2005/2 -> additional provisions for **business continuity management** (inter alia for credit institutions and stockbroking firms)
- NBB_2019_09 -> establishes the **reporting** on **operational** and **security risks** of payment services to be submitted by **credit institutions** and branches of credit institutions
- NBB_2020_24 -> establishes the **reporting** on **operational** and **security risks** of payment services to be submitted by **payment institutions** and **electronic money institutions**

EBA statement on additional supervisory measures in the COVID-19 pandemic

- https://eba.europa.eu/coronavirus -> Statement 22/04/'20 -> Section "Digital operational resilience"

Situation	Institutions face **additional challenges** (business continuity, security)
	Affirms **importance** of **operational resilience** (and of the EBA Guidelines)
Financial institutions	Ensure **internal governance/internal control framework/risk management** for operational resilience
	Take measures to **ensure capacity** of IT systems to support most critical activities (e.g. **remote working**)
	Stay vigilant in their **cyber security monitoring** and **measures**
	Ensure **effective crisis communication** measures with all relevant stakeholders
	Monitor and seek assurance on the **level of compliance** of **third party providers**
	Ensure that the **business continuity plans** are **up to date** and **adapted**
Competent authorities	Ensure **effective prioritisation** of efforts -> focus on **information security**, **ICT operations** and **business continuity** management
	Apply **reasonable supervisory flexibility** when assessing the implementation of the Guidelines

Overview

- IT prudential supervision NBB
- EBA Guidelines on ICT/cyber risk management
  - Integration in NBB policy framework
  - Content guidelines/public consultation
- Q&A

EBA GUIDELINES ON ICT AND SECURITY RISK MANAGEMENT

EBF Cybersecurity Working Group, Brussels | 14 February 2020

Vaidotas Tamulenas

Bank Expert | Banking Markets, Innovation and Products | EBA

Setting the scene

Cybersecurity should be undertaken as part of a financial institution's overall information security risk management…

…but cyber-attacks have some specific characteristics which should be taken into account in ensuring that the information security measures are adequate to mitigate cyber risks:

→ malicious cyber-attacks are often **difficult to identify**, fully **eradicate**, and **determine** damage;

→ some cyber-attacks can render common risk management and business continuity arrangements **ineffective**;

→ third party service providers, vendors and vendors' products may become **channels to propagate** cyber-attacks.

ICT and security risk management is fundamental for a financial institution to achieve its **strategic**, **corporate**, **operational** and **reputational** objectives

EBA Guidelines on ICT and security risk management

"**ICT and security risk** – risk of loss due to breach of **confidentiality**, failure of **integrity** of systems and data, inappropriateness or **unavailability** of systems and data or inability to change information technology (IT) within a reasonable time and with reasonable costs when the environment or business requirements change (i.e. agility). This includes security risks resulting from inadequate or failed internal processes or external events including cyber-attacks or inadequate physical security. "

Addressees:

payment service providers (PSPs)	for provision of payment services
credit institutions	for all activities beyond their payment services
investment firms	for all activities

- GL integrate '*Guidelines on security measures for operational and security risks of payment services*' (EBA/GL/2017/17), **addressed to PSPs, and only for their payment services**, issued in 2017, to repealed from the date of application of ICT Guidelines.
- GL to be read in conjunction with:
  - ✓ the *EBA Guidelines on ICT risk assessment under the Supervisory Review and Evaluation Process* (EBA/GL/2017/05)
  - ✓ the *EBA Guidelines on outsourcing arrangements* (EBA/GL/2019/02)

Outcome of public consultation

Public consultation: December 2018 – March 2019. 30 industry responses addressed.

- Less-prescriptive, more **principle-based guidance**
- **Technology and methodology agnostic** *(financial institutions should refer to existing standards and leading best practices)*
- **Risk-based** approach
- Implementation should be done in accordance with the principle of **proportionality:**
  - Financial institutions' size, their internal organisation
  - Nature, scope and complexity of services and products
  - Riskiness of related processes and services

EBA Guidelines on ICT and security risk management apply from 30 June 2020

Public consultation (further detail)

- Principle based:
  - Refrain from being **too prescriptive** (**"what"** to achieve, not **"how"**)
  - **Removal** of **detailed processes/implementation aspects** (e.g. **Agile** development, **change management** process)
  - Link more clearly to **pre-existing guidance**, **international practices**, **standard**, etc.?
    - **FSB** lexicon, other **EBA guidelines** (outsourcing, internal governance), …
    - But remain **methodology** (technology) **agnostic** (ISO, NIST, etc.)
    - Sufficiently principle based -> **no inconsistencies**
- Proportionality/risk based:
  - Ambition to be **"size neutral"**
  - To **prioritize efforts** where they are mostly needed
  - **Not** a ground for **exemption**

Public consultation (further detail) (continued)

- Clarifications/change on wording/definitions (e.g. incident, asset, action plan, data life cycle, risk appetite, independent testers, project governance, external data, short/long term, etc.)
- Clarifications/changes/confirmation on content (non-exhaustive):
  - Role 2nd line and positioning of "information security function":
    - Alignment EBA guidelines on internal governance
    - Variety of institutions/implementations -> not too prescriptive
    - Emphasis on roles (e.g. monitoring and controlling adherence), not on functions (e.g. CISO)
    - Appropriate segregation of ICT operations, control, and internal audit functions
  - Role management body in approving (e.g. risk management framework, audit plan, information security policy, processes/procedures)
  - Monitoring all activities by privileged users
  - Implementation of secure configuration baselines of all network components
  - Encryption in accordance with the data classification

Public consultation (further detail) (continued)

- **Testing** (source code reviews, vulnerability assessments, red teaming, penetration testing) **should be proportionate/commensurate** to **risk exposure** and **maturity of security risk management**
- Conducting **security tests** on a risk-based approach but **at least every 3 years** (non-critical systems)
- Periodic **security awareness programmes** and at least annual **training** for all staff **and contractors**
- The **inventory** should contain **all assets**, which then need to be classified for criticality
- **Obligation to patch** cannot be removed in the case of a **critical system**
- **Backups** stored securely/sufficiently remote from primary site, i.e. **not exposed to the same risks**
- Handle the **changes during emergencies** following procedures that provide adequate safeguards
- **BIAs** should **cover 3rd parties**
- **Criticality assessment** needs to **include** the **supporting processes** and **information assets**
- **Testing switch-over** of **critical business functions** is **necessary**
- **Testing of third party** information assets and interdependencies, where applicable

An overview

EBA GUIDELINES ON ICT AND SECURITY RISK MANAGEMENT

Governance

Governance

The **management body** ensure an adequate internal governance and internal control framework in place for their ICT and security risks:

- set clear **roles** and **responsibilities** (for the management body and its committees)
- ensure adequate **quantity** and **skills** of financial institutions' **staff**
  - ✓ all staff members, including key function holders, to receive appropriate training on ICT and security risks (annually or more frequently)
- ensure appropriate allocated **budget**

The **management body** has overall **accountability** for **setting**, **approving** and **overseeing** the implementation of financial institutions' **ICT strategy** as part of their overall business strategy as well as for the establishment of an effective **risk management framework** for ICT and security risks

Strategy and use of third parties

Strategy

The **ICT strategy** aligned with overall **business strategy**:

- ICT to effectively support and participate in business strategy, including the evolution of the **organisational structure**, **ICT system changes** and **key dependencies with third parties**
- Clear information security objectives on ICT **systems** and ICT **services**, **staff** and **processes**

Use of third party providers

Ensure **effectiveness of the risk mitigating measures** when operational functions of payment services and/or ICT services and ICT systems of any activity are **outsourced** / **using third parties**

Contracts and **service level agreements** (*normal circumstances + event of service disruption*):

- ✓ minimum **cybersecurity requirements**
- ✓ specifications of **data life cycle**
- ✓ **data encryption** requirements
- ✓ **network security** and **security monitoring** processes
- ✓ **location of data centres**
- ✓ operational and security **incident handling procedures** (escalation and reporting)

ICT and security risk management framework (1)

Processes of ICT and security risk management framework in place to:

- determine the **risk appetite** for ICT and security risks, in accordance with the risk appetite
- identify and assess the **ICT and security risks** to which financial institutions are exposed
- define **mitigation measures**, including controls, to mitigate ICT and security risks
- monitor the **effectiveness** of these measures, the number of reported incidents, affecting the ICT-related activities, and take actions to **correct the measures** where necessary
- report to the management body on the **ICT and security risks** and **controls**
- identify and assess any ICT and security risks resulting from any **major change** in ICT system or ICT services, processes or procedures, and/or after **any significant operational or security incident**

Financial institutions should ensure that the ICT and security risk management framework is **documented**, and **continuously improved,** based on **'lessons learned'** during its implementation and monitoring. The ICT and security risk management framework should be **approved and reviewed**, at least once a year, by the management body.

ICT and security risk management framework (2)

Identification of functions, processes and assets

- Identify, establish and maintain **updated mapping** of **business functions**, **roles** and **supporting processes** to identify the importance of each and their interdependencies related to ICT and security risks
- Identify, establish and maintain an **updated mapping** of the **information assets** supporting their **business functions and supporting processes** *[such as ICT systems, staff, contractors, third parties and dependencies on other internal and external systems and processes]* to be able to, **at least**, manage the information assets that support their **critical** business functions and processes.

Classification and risk assessment

BF, SP, IA = business functions, supporting processes and information assets

- **Classify** the identified **BF, SP, IA** in terms of **criticality** *(confidentiality, integrity, availability requirements*). Clearly assign **accountability** and **responsibility** for the information assets
- Identify the ICT and security risks that impact identified and classified **BF, SP, IA**, according to their criticality. **Risk assessment** should be carried out and documented **annually** or **at shorter intervals** if required (e.g. on any major changes in infrastructure, processes or procedures)
- Ensure **continuous monitoring** of threats and vulnerabilities relevant to their **BF, SP, IA** and regularly review the risk scenarios impacting them

ICT and security risk management framework (3)

Risk mitigation

- Based on the risk assessments, determine which **measures** are required to **mitigate** identified risks to **acceptable levels** and whether **changes are necessary** to the existing **business processes**, **control measures**, ICT **systems** and ICT **services**
- Consider the **time** required **to implement** these changes and the **time** to take **appropriate interim mitigating measures** to minimise risks to stay within ICT and security risk appetite

Reporting

- Report risk assessment results to the management body in a **clear** and **timely manner**

Audit

- **Governance**, **systems** and **processes** for ICT and security risks should be periodically audited
- The **frequency** and **focus** commensurate with the relevant ICT and security **risks;** management body to approve the audit plan
- Auditors should have sufficient **knowledge**, **skills** and **expertise** in ICT and security risks (and in payments (for PSPs); **be independent** within or from the financial institution
- A **formal follow-up process** – provisions for the **timely verification** and **remediation** of critical ICT audit findings

Information security policy

Develop and document an **information security policy** to define the **high-level principles** and rules to protect the **confidentiality**, **integrity** and **availability** of financial institutions' and their customers' **data** and **information**

- **in line with** financial institutions' **information security objectives**
- **based on** the relevant results of the **risk assessment process**
- **approved** by the management body

- ✓ Describe the main **roles** and **responsibilities** for **information security management**
- ✓ Set out **requirements for staff** and **contractors**, **processes** and **technology** in relation to information security (recognise that staff and contractors **at all levels** have responsibilities)
- ✓ Ensure the **confidentiality**, **integrity** and **availability** of financial institutions' **critical** logical and physical assets, resources and sensitive data whether **at rest**, **in transit** or **in use**
- ✓ Be **communicated** to **all staff and contractors**

- Based on the information security policy, **establish** and **implement** **security measures** to mitigate the ICT and security risks that they are exposed to

Security measures to mitigate the ICT and security risks

Governance

Logical security

Physical security

ICT operations security

Security monitoring

Information security reviews, assessment and testing

Information security training and awareness

Financial institutions to identify and manage their ICT and security risks:

- **Operations**. The ICT function(s) **in charge** of ICT systems, processes and security operations should have appropriate processes and controls to ensure that (i) all risks are **identified**, **analysed**, **measured**, **monitored**, **managed**, **reported** and **kept within the limits** of the **risk appetite;** (ii) projects and systems delivered and activities performed are in **compliance** with external and internal requirements
- **Control function**. Responsibility for **managing and overseeing** ICT and security risks. Ensure **independence** and **objectivity** by **appropriate segregation** from ICT operations processes. Directly **accountable** to the **management body** and **responsible** for **monitoring and controlling adherence** to the ICT and security risk management framework. Ensure that ICT and security risks are **identified**, **measured**, **assessed**, **managed**, **monitored** and **reported**. Control function **not to be responsible** for internal audit.
- **Internal audit function**. Follow a risk-based approach, capacity to **independently review and provide objective assurance** of the **compliance** of all ICT and security-related activities and units of a financial institution with the financial institution's policies, procedures, external requirements.

Security measures to mitigate the ICT and security risks

- Governance
- **Logical security**
- Physical security
- ICT operations security
- Security monitoring
- Information security reviews, assessment and testing
- Information security training and awareness

- **Define**, **document** and **implement** procedures for logical access control (identity and access management)
- These procedures should be **implemented**, **enforced**, **monitored** and periodically **reviewed**. Include controls for monitoring anomalies
- At a minimum, implement the following elements:
  - ✓ Need-to-Know, Least Privilege and Segregation of Duties
  - ✓ User accountability
  - ✓ Privileged access rights
  - ✓ Logging of user activities
  - ✓ Access management
  - ✓ Access recertification
  - ✓ Authentication methods
- Electronic access by applications to data and ICT systems should be limited to a minimum required to provide the relevant service

Security measures to mitigate the ICT and security risks

- Governance
- Logical security
- **Physical security**
- ICT operations security
- Security monitoring
- Information security reviews, assessment and testing
- Information security training and awareness

- Physical security measures should be defined, documented and implemented to **protect** **premises, data centres** and **sensitive areas** from **unauthorised access** and from **environmental hazards**
- Physical access to ICT systems should be permitted to **only authorised individuals**
- Authorisation should be assigned in accordance with the individual's **tasks and responsibilities** and limited to individuals who are appropriately **trained and monitored**
- Physical access should be regularly reviewed to ensure that unnecessary access rights are **promptly revoked** when not required
- Adequate measures to protect from environmental hazards should be commensurate with the **importance of the buildings** and the **criticality of the operations** or **ICT systems** located in these buildings

Security measures to mitigate the ICT and security risks

- Governance
- Logical security
- Physical security
- **ICT operations security**
- Security monitoring
- Information security reviews, assessment and testing
- Information security training and awareness

- Implement procedures to **prevent occurrence** of security issues in ICT systems and ICT services, and **minimise their impact** on ICT service delivery:
  - ✓ identification of **potential vulnerabilities,** which should be evaluated and remediated by ensuring that **software and firmware are up-to-date** *(incl. software provided to internal and external users)* by **deploying critical security patches** or implementing **compensating controls**
  - ✓ implementation of **secure configuration** baselines of all network components
  - ✓ implementation of **network segmentation, data loss prevention systems** and the **encryption of network traffic** (based on the data classification)
  - ✓ implementation of **protection of endpoints** including servers, workstations and mobile devices. Evaluate whether endpoints meet defined security standards before they are granted access to the corporate network
  - ✓ mechanisms to **verify the integrity** of software, firmware, and data
  - ✓ **encryption of data** at rest and in transit (based on the data classification)
- On an on-going basis determine whether **changes in the existing operational environment** influence the **existing security measures** or require **adoption of additional measures** to mitigate related risks appropriately

Security measures to mitigate the ICT and security risks

- Governance
- Logical security
- Physical security
- ICT operations security
- **Security monitoring**
- Information security reviews, assessment and testing
- Information security training and awareness

- Establish and implement policies and procedures to **detect anomalous activities** that may impact information security, and to **respond** to these events appropriately
- Implement **appropriate and effective** capabilities for detecting and reporting **physical or logical intrusion** as well as **breaches of confidentiality**, **integrity** and **availability** of the information assets. The continuous monitoring and detection processes should cover:
  - ✓ **relevant internal and external factors**, including business and ICT administrative functions
  - ✓ **transactions** to detect misuse of access by third parties or other entities and internal misuse of access
  - ✓ **potential** internal and external **threats**
- Establish and implement processes and organisation structures to identify and constantly **monitor security threats** that could materially affect their ability to provide services. **Actively monitor technological developments** to be aware of security risks. Implement **detective measures** (*to identify possible information leakages, malicious code and other security threats, and publicly known vulnerabilities in software and hardware*), check for corresponding **new security updates**.

Security measures to mitigate the ICT and security risks

- Governance
- Logical security
- Physical security
- ICT operations security
- Security monitoring
- **Information security reviews, assessment and testing**
- Information security training and awareness

✓ May perform **gap analysis**, **compliance reviews**, internal and external **audits** of the information systems, or **physical security reviews**

✓ Should consider good practices such as **source code reviews**, **vulnerability assessments**, **penetration tests** and **red team exercises**

✓ Tests to be carried out by **independent testers** with sufficient knowledge, skills and expertise, and **not involved in the development** of the information security measures

✓ Include **vulnerability scans** and **penetration tests** (threat-led penetration testing where necessary and appropriate) commensurate to the level of risk

- Conduct tests of security measures in the event of:
  - changes to infrastructure, processes or procedures
  - because of major operational or security incidents
  - release of new/ significantly changed internet-facing critical applications
- Monitor and **evaluate results** of the security tests, and **update** security measures accordingly **without undue delays** in case of critical ICT systems

For all **critical ICT systems** these tests shall be performed at least **on an annual basis**. **Non-critical systems** should be tested **regularly** using **risk-based approach**, but at least **every 3 years.**

Security measures to mitigate the ICT and security risks

- Governance
- Logical security
- Physical security
- ICT operations security
- Security monitoring
- Information security reviews, assessment and testing
- **Information security training and awareness**

Financial institutions should establish:

- **a training programme**
- including periodic **security awareness programmes:**
  - ✓ for **all staff and contractors** to ensure that they are trained to perform their duties and responsibilities consistent with the relevant security policies and procedures
  - ✓ to reduce **human error**, **theft**, **fraud**, **misuse** or **loss**
  - ✓ to know how to address information security related risks
- Financial institutions should ensure that the training programme provides **training for all staff members** and **contractors** **at least annually**

ICT operations management

"Financial institutions should manage their ICT operations based on **documented** and **implemented** processes and procedures that are **approved** by the management body."

Documented and implemented processes and procedures

- Align to business requirements
- Minimise potential errors from manual tasks
- Logging and monitoring for critical operations
- Up-to-date inventory of ICT assets
- Monitor and manage lifecycle of ICT assets
- Performance and capacity planning & monitoring
- ICT systems backup and restoration procedures

ICT project management

- Programme/project governance process
- Monitor and mitigate risks
- ICT project management policy:
  - ✓ Project objectives
  - ✓ Roles and responsibilities
  - ✓ Project risk assessment
  - ✓ Project plan, timeframe, steps
  - ✓ Key milestones
  - ✓ Change management requirements

Incident and problem management

- Identify, track, log, categorise and classify incidents
- Roles and responsibilities for different incidents
- Identify, analyse and solve the root cause
- Internal communication plans
- Incident response procedures to mitigate impact
- Specific external communication plans

ICT systems acquisition and development

- ✓ Risk based approach
- Clear functional & non-functional requirements
- Unintentional alteration / intentional manipulation
- Testing methodology (consider criticality)
- Separate ICT environments: *production* vs *development, testing, other non-production*
- Proper documentation (reduce dependency on subject matter expert)

ICT change management

Record, test, assess, approve, implement and verify all changes to ICT systems in a controlled manner

Business continuity management

"Financial institutions should establish a sound business continuity management process to maximise their abilities to provide services on an on-going basis and to limit losses in the event of severe business disruption"

Business impact analysis (BIA):

- Analyse exposure to severe disruptions
- Assess potential impact (quant. & qual.)
  - ✓ Confidentiality
  - ✓ Integrity
  - ✓ Availability
- Internal and/or external data, scenarios
- Consider the criticality of BF, SP, IA

Response and recovery plans

- Based on BIA and plausible scenarios, develop **response and recovery plans**
- Specify conditions to prompt activation
- Specify actions to ensure availability, continuity and recovery of, at least, critical ICT systems and ICT services
- Short-term / long-term recovery options
- Continuity measures to mitigate failure of key importance third party provider

Business continuity planning

Based on BIA, establish **business continuity plans** (BCP):

- Documented and approved by management body
- React to potential failure scenarios
- Recover operations of critical business activity within
  - ✓ Recovery Time Objective (time to restore)
  - ✓ Recovery Point Objective (acceptable data loss)
- Prioritise actions in case severe disruption (risk-based approach)
- Consider a range of different scenarios

Testing of plans

BCPs critical business functions, supporting processes, information assets and their interdependencies (including provided by third parties) tested at least annually

- adequate set of severe but plausible scenarios
- challenge the assumptions on which BCPs rest
- verify the ability to respond

Crisis communication

Timely and appropriately inform all relevant internal and external stakeholders (incl. CA if required)

Payment service user relationship management

Applies only to payment service providers (PSPs) for their provision of payment services

- ✓ PSPs to enhance payment service users' **awareness of security risks** (new threats and vulnerabilities)
- ✓ Where product functionality permits, allow to **disabling specific payment functionalities**
- ✓ Option to adjust **spending limits for payment transactions**
- ✓ Option to receive **alerts on initiated and/or failed attempts** to initiate payment transactions
- ✓ Inform about **updates in security procedures**
- ✓ Provide **assistance** related to payment services

Contact

Should you have any further questions do not hesitate to contact:

Vaidotas Tamulenas

Bank Expert | Banking Markets, Innovation and Products

https://eba.europa.eu/financial-innovation-and-fintech/fintech-knowledge-hub
EUROPLAZA, 20 Avenue André Prothin
92927 Paris La Défense, France
Direct tel: +33 (0) 1 86 52 70 19
E-mail: Vaidotas.Tamulenas@eba.europa.eu

EUROPEAN BANKING AUTHORITY

Floors 24-27, 20 Av André Prothin, 92927 Paris La Défense

Tel: +33 1 86 52 7000

E-mail: info@eba.europa.eu

http://www.eba.europa.eu

Overview

- IT prudential supervision NBB
- EBA Guidelines on ICT/cyber risk management
  - Integration in NBB policy framework
  - Content guidelines/public consultation
- Q&A

Q&A

Contact NBB:

Thomas Plomteux

Head of IT Prudential Supervision (dep: Surveillance of financial market infrastructures, payment services and cyber risks)

E-mail: Thomas.Plomteux@nbb.be

Direct tel: +32 (0)2 221 21 97