FIGI Security Clinic

- Risks in Digital Financial Services
- Cyber resilience for Financial Market Infrastructures

FIGI FINANCIAL INCLUSION GLOBAL INITIATIVE

Dorothee Delort, WB

4-5 December 2019
#financialinclusion

Sponsored by

BILL & MELINDA GATES foundation

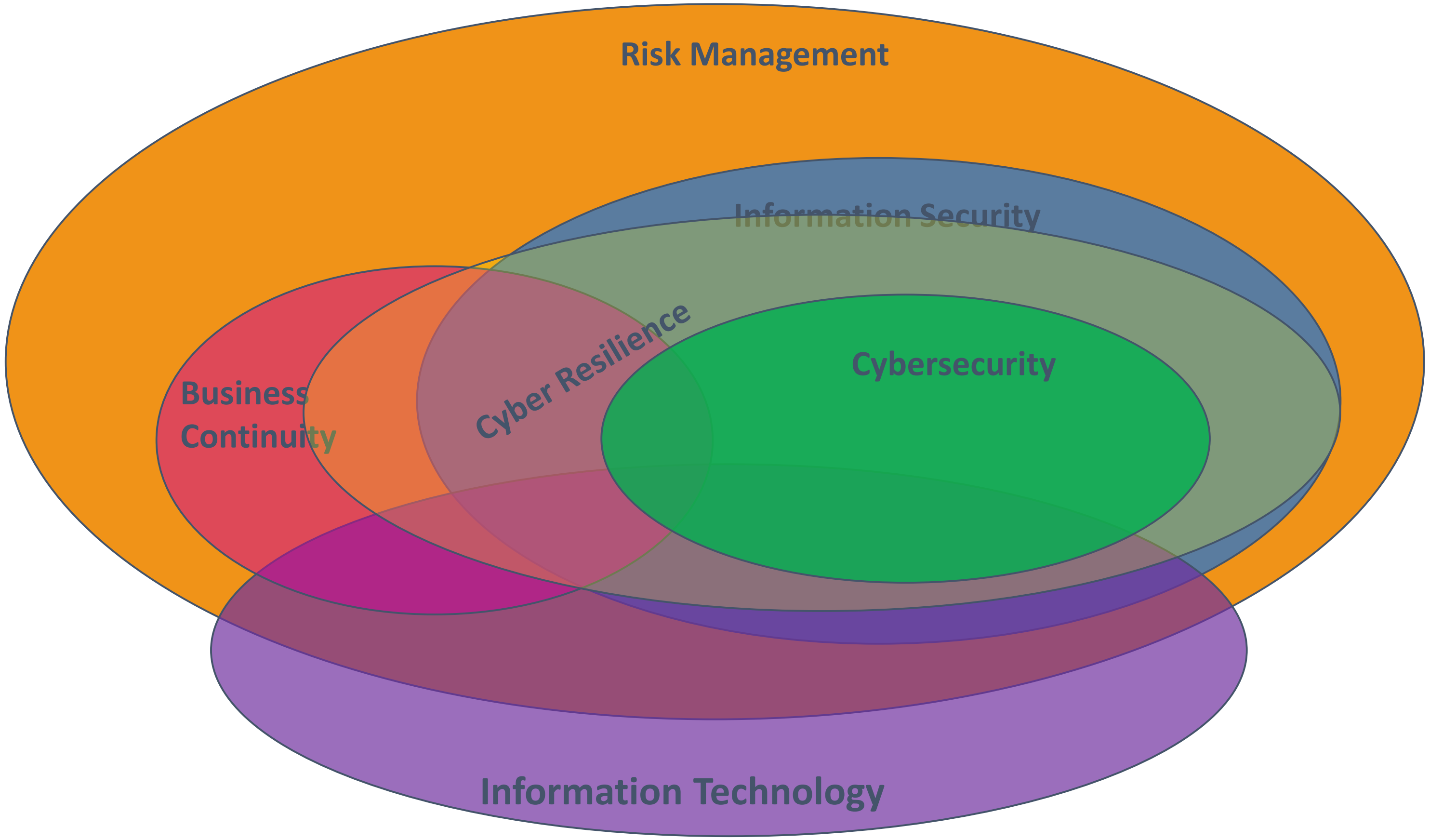
Organized by

Committee on Payments and Market Infrastructures
BANK FOR INTERNATIONAL SETTLEMENTS

WORLD BANK GROUP

ITU

A dynamic context where the scope of each activity continuously changes…

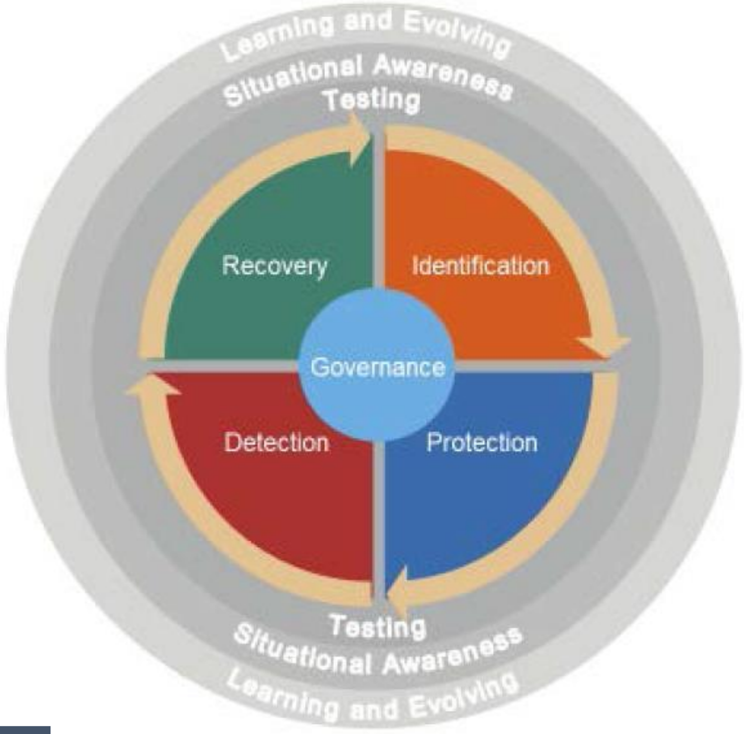


CPMI-IOSCO Guidance on Cyber Resilience for FMI

The Guidance is structured in chapters defining five main risk management categories and three general components that should be considered when talking about cyber resilience applied to FMI.

- Risk management categories are:
  - i. Governance
  - ii. Identification
  - iii. Protection
  - iv. Detection
  - v. Recovery

- General components are:
  - i. Test
  - ii. Situational awareness
  - iii. Learning and Evolution



Cyber Resilience Oversight Expectations – December 2018

https://www.bis.org/cpmi/publ/d146.pdf

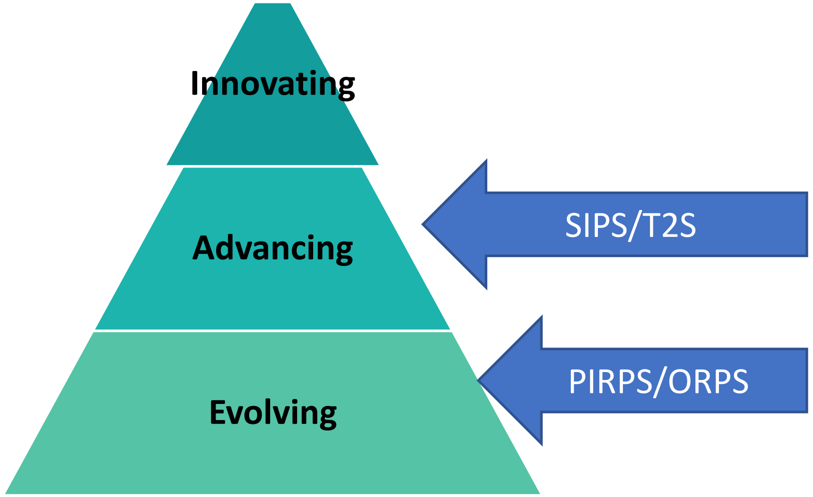
FIGI & ECB Cyber Resilience Oversight Expectations (CROE)

CROE – why?

- Sets up a more detailed elaboration of the CPMI-IOSCO Cyber Guidance to aid FMIs and overseers in implementing the Guidance and assessing the FMI's compliance against it
- Provides good practices which can be referred to when giving feedback to FMIs regarding assessments in the future
- Takes into consideration the industry best practices, already set out in different frameworks – e.g. *FFIEC Cybersecurity Assessment Tool, the NIST Cybersecurity Framework, ISF Standard of Good Practice, COBIT and ISO/IEC 27001*
- Provides the basis for overseers to work with FMIs over longer term to raise the FMI's maturity level
- Can be used as:
    - Assessment Methodology for overseers; and
    - Tool for self-assessments for FMIs.

Levels of expectations: the three-level approach

- Based on the ***three level*** approach;
- Each chapter is divided into the three levels of expectations;



- Applied in order to *adapt* to a changing cyber environment;
- FMIs are expected to *continuously evolve* on the cyber maturity scale;
- Provide an *insight* about the FMI's level of cyber resilience and what it needs to improve in terms of cyber expectations;
- Takes into account the *proportionality* principle

Cyber Resilience Oversight Expectations (CROE)

Levels of expectations: the three-level approach

Evolving level

- Essential capabilities are established and sustained across the FMI to identify, manage and mitigate cyber risks, in alignment with the approved cyber resilience strategy and framework, and
- performance of practices is monitored and managed.

- **All payment systems must meet the Evolving Expectations, aspiring to move to Advancing level**

Advancing level

- Evolving level *Plus*
- practices incorporate more advanced implementations that have been improved over time, and
- capabilities are harmonized across the FMI to proactively manage cyber risks to the enterprise.

- **All SIPS must meet the Advancing Expectations, aspiring to move to Innovating level**

Innovating level

- Evolving level *Plus*
- Advancing level *Plus*
- capabilities across the FMI are enhanced as needed, in the midst of the rapidly evolving cyber threat landscape, to strengthen the cyber resilience of the FMI and its ecosystem, by proactively collaborating with its external stakeholders;

Cyber Resilience Oversight Expectations (CROE)

1. Governance and Continuous Evolution
2. Identification & Situational Awareness
3. Protection
4. Detection
5. Response and Recovery

Conclusion - Key messages

- To reach and evolve to high levels of cyber resilience for FMIs:
  - A **continuous monitoring** of **new trends in cyber attacks** and **update** of **defence mechanisms** are key
  - Focus not only **technology**, but consider also **processes** and **people**
  - Design, test, implement and update both **preventive, detective** and **reactive** controls.
  - Do **not forget 4** crucial elements as:
    - **The establishment of a proper governance**
    - **The identification and prioritization of risks**
    - **Use of an established framework**
    - **The risk stemming from third parties and new technologies must be identified and managed**