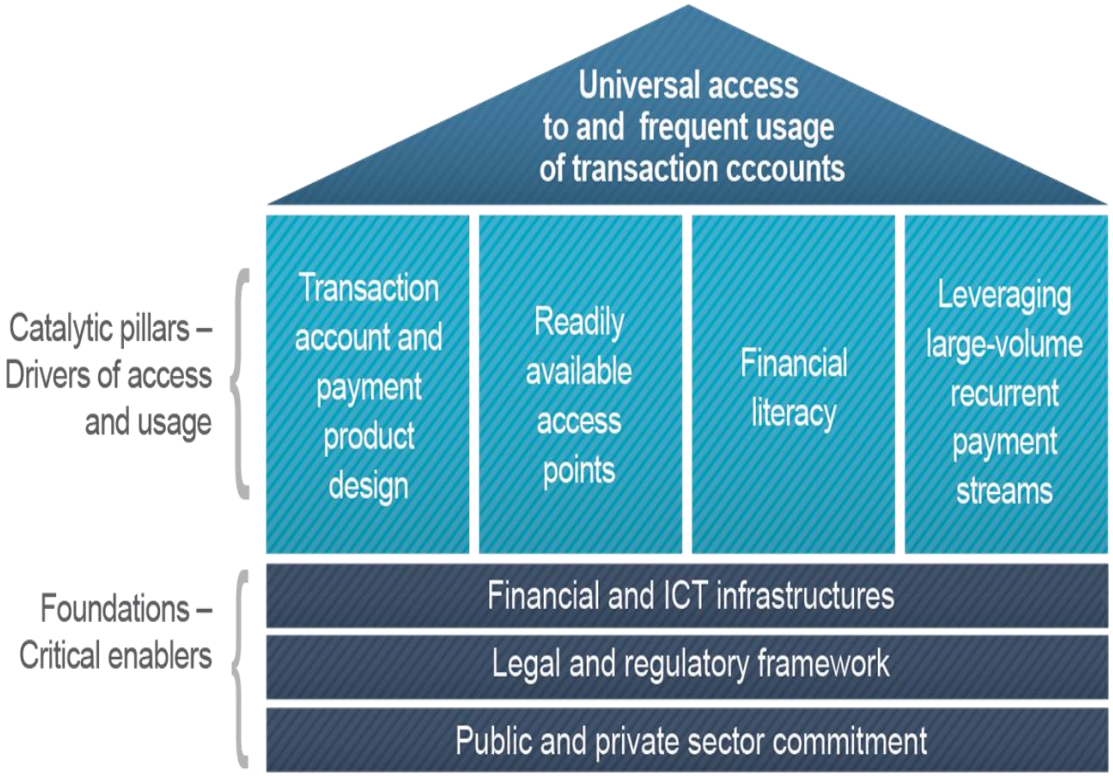
Interoperability and resiliency requirements of Digital Payments System

DOROTHEE DELORT
PAYMENT SYSTEMS DEVELOPMENT GROUP, WORLD BANK



The WBG work on foundations for digital payments and financial inclusion



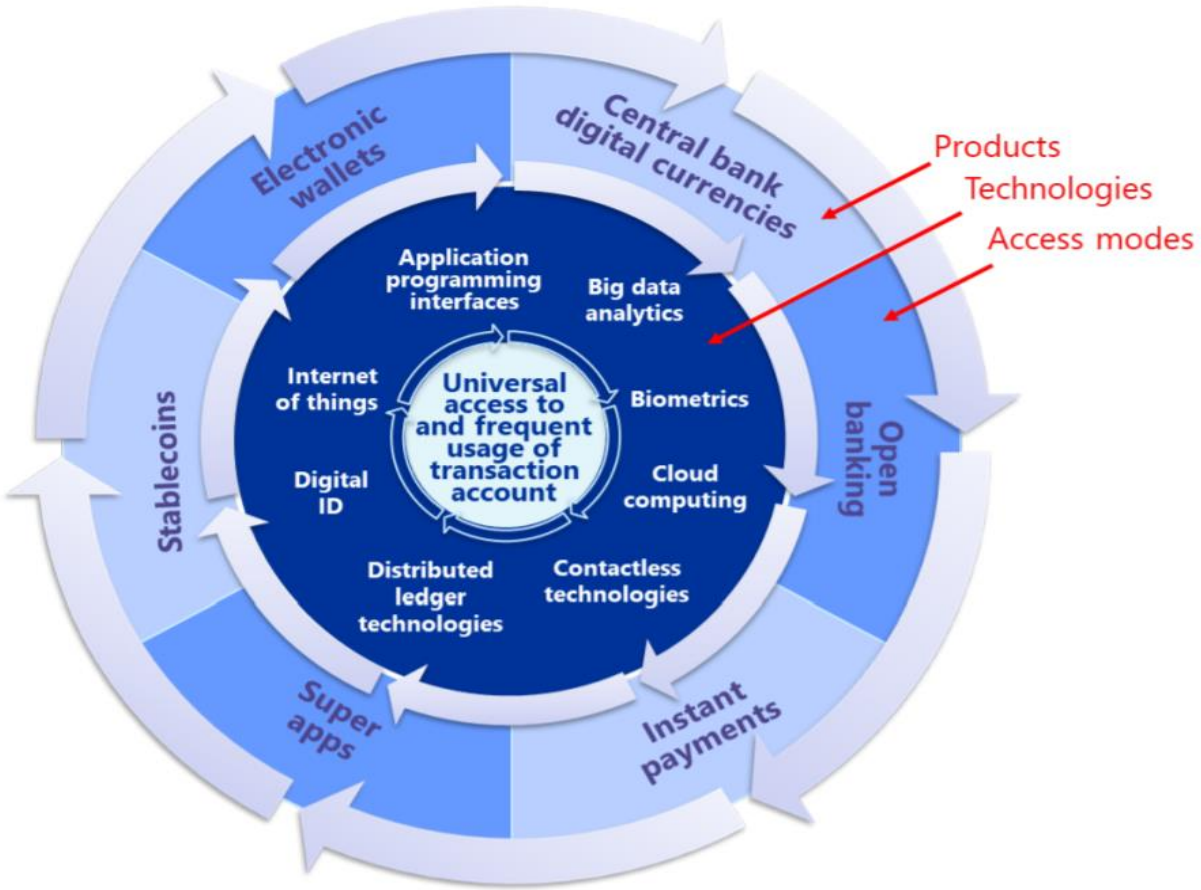
Data / Analytics

Knowledge Sharing / Advocacy

Operational / country work & diagnostics

WORLD BANK GROUP	• **Global Findex** • **Focused surveys** (Payments, Consumer Protection, Financial Capability, Remittances)	• **WB Research** / Impact Evaluations • **Diagnostics**, policy toolkits • **We-Fi –** knowledge sharing on financing women entrepreneurs	• **National Financial Inclusion Strategies** • **WB Advisory and Lending** • **IFC Advisory and Investments** • **IDA18 Commitments** for financial inclusion and gender • **FSAP** • **FIRST**

The WBG work on Fintech for digital payments and DFS



CPMI-IOSCO Principles for Financial Market Infrastructures (PFMIs)

Categorized into 9 broad categories:

- *General organization:* P 1, 2, 3
- *Credit and liquidity risk management:* P 4, 5, 6, 7
- *Settlement:* P 8, 9, 10
- *Central securities depositories and exchange-of-value settlement systems:* P 11, 12
- *Default management:* P 13, 14
- *General business and operational risk management:* P 15, 16, 17
- *Access:* P 18, 19, 20
- *Efficiency:* P 21, 22
- *Transparency:* P 23, 24

Fostering interoperability

- *Legal framework and system rules*
- *Access:* P 18, 19, 20
- Governance: P 2
- *Efficiency:* P 21, 22
- *Transparency:* P 23, 24

- Catalyst role of the Central Bank

- Cooperation and dialogue with the stakeholders

Building resiliency

- *Legal resilience: P 1*
  - *Settlement:* P 8, 9, 10
- *Organizational resilience: P* 2, 3
- *Financial resilience: Credit and liquidity risk management:* P 4, 5, 6, 7
- *Resilience in situation of default:* P 13, 14
- *General business resilience: P 15*
- *Operational resilience:* P 17

Building resiliency

- *Legal resilience: P 1*
  - *Settlement:* P 8, 9, 10
- *Organizational resilience: P* 2, 3
- *Financial resilience: Credit and liquidity risk management:* P 4, 5, 6, 7
- *Resilience in situation of default:* P 13, 14
- *General business resilience: P 15*
- *Operational resilience:* P 17

Principle 17: Operational risk

An FMI should identify the plausible sources of operational risk, both internal and external, and mitigate their impact through the use of appropriate systems, policies, procedures, and controls. Systems should be designed to ensure a high degree of security and operational reliability and should have adequate, scalable capacity. Business continuity management should aim for timely recovery of operations and fulfilment of the FMI's obligations, including in the event of a wide-scale or major disruption.

✓ PS	✓ CSD	✓ SSS	✓ CCP	✓ TR

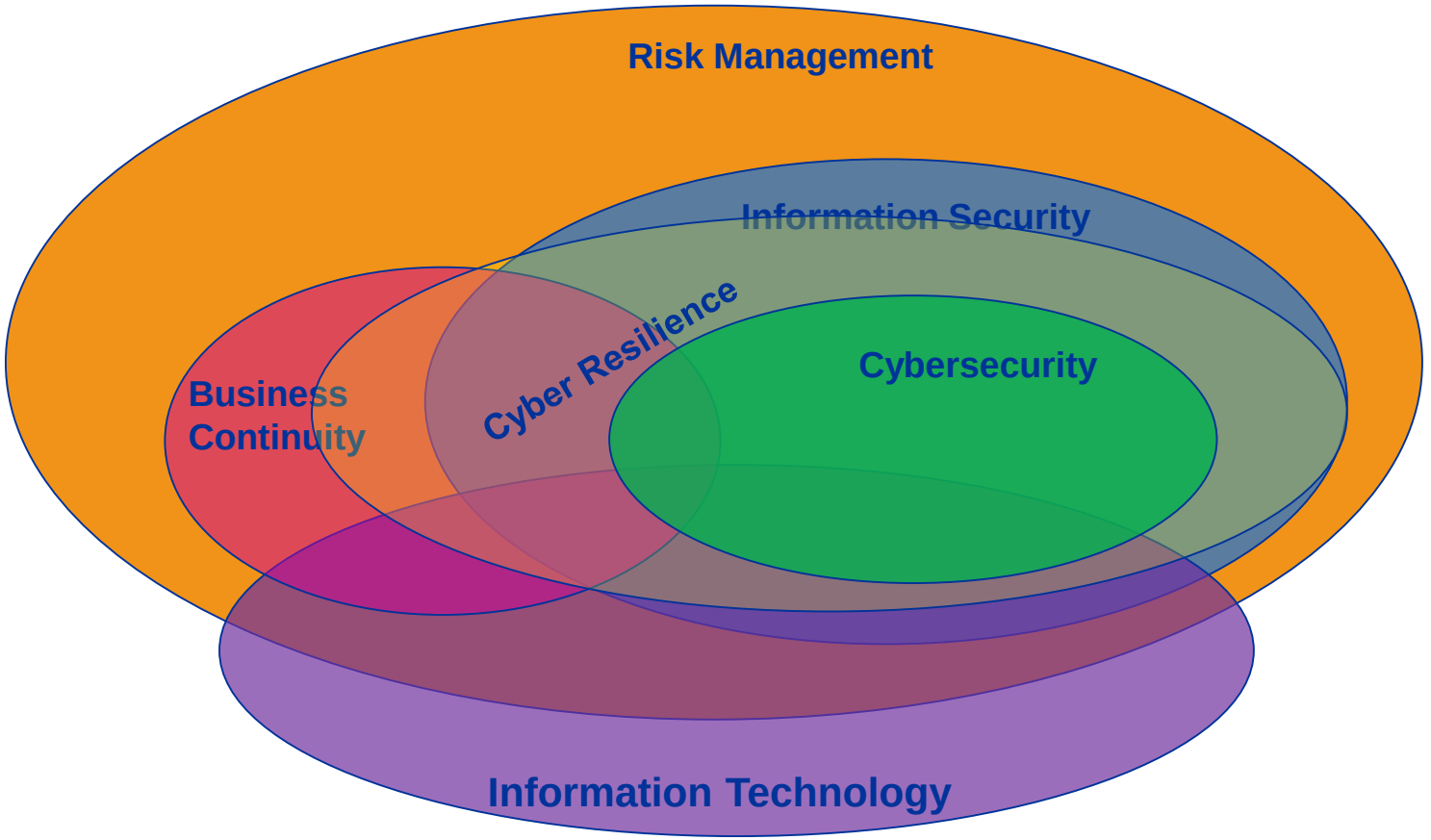
- ***Key considerations:***

- Establish a robust operational risk-management framework to identify, monitor, and manage operational risk
- Have clearly defined roles and responsibilities for addressing operational risk; test systems and operational policies, procedures, and controls periodically and after significant changes
- Have clearly defined operational reliability objectives and policies to achieve those objectives

Principle 17: Operational risk

- ***Key considerations:***
- Have scalable capacity to handle increasing stress volumes and to achieve service-level objectives
- Have comprehensive physical and information security policies
- Develop a comprehensive business continuity plan (BCP) to handle a wide-scale or major disruption; the plan should:
  - incorporate the use of a secondary site
  - ensure critical IT systems can resume operations within two hours following disruptive events
  - enable the FMI to complete settlement by the end of the day of the disruption, even in extreme circumstances
  - review and test regularly the BCP arrangements
- Identify, monitor, and manage risks that participants, other FMIs, and service and utility providers pose to its operations and the risks its operations pose to other FMIs

Cyber resilience of Financial Market Infrastructures



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

ECB Cyber Resilience Oversight Expectations – December 2018

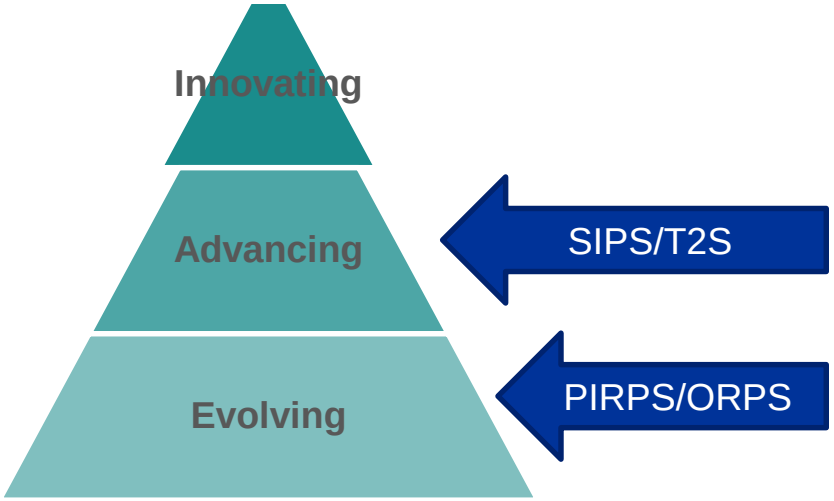
https://www.bis.org/cpmi/publ/d146.pdf

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 (specific minimum requirements for SIPS/T2S, PIRPS, ORPS).

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**

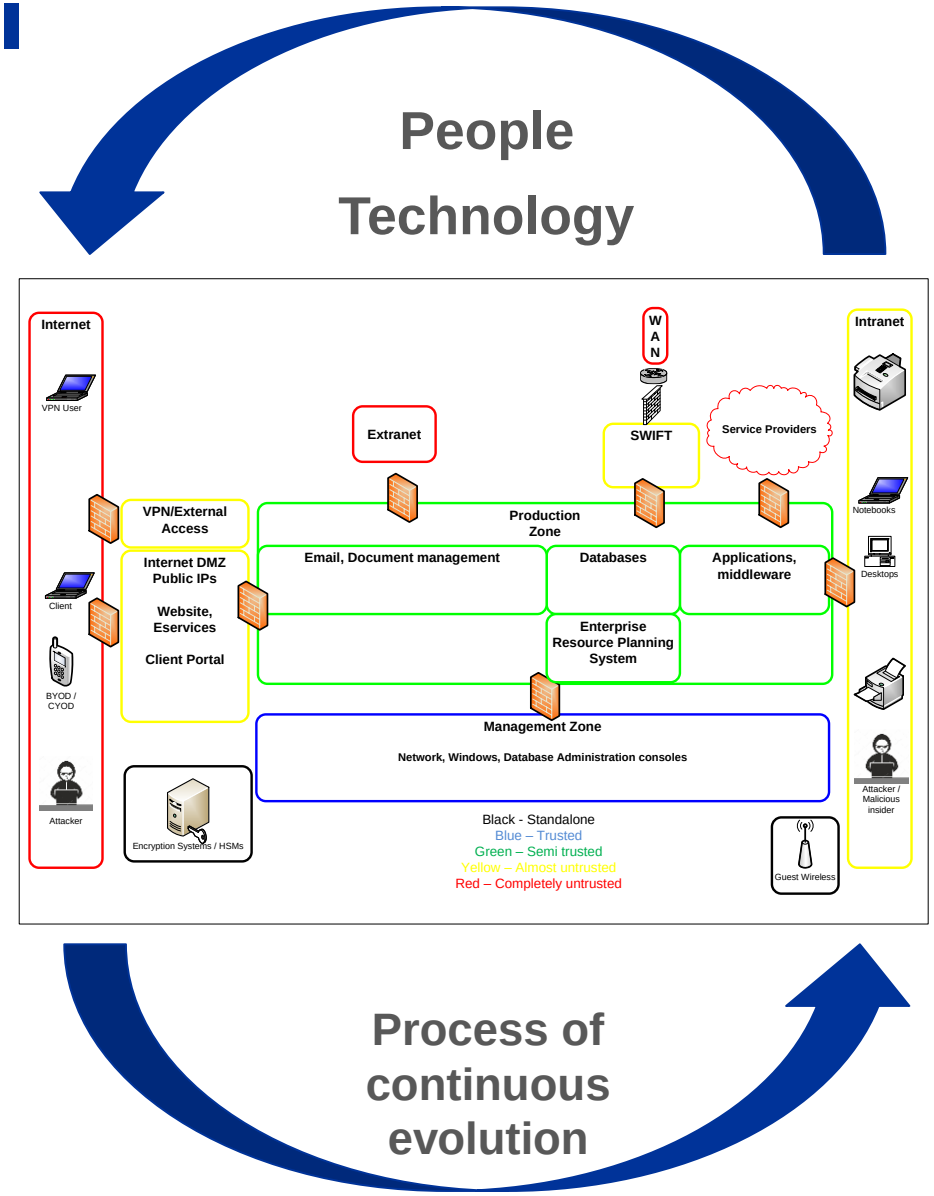
Innovating level

- 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 in FMI

The CROE covers the following topics and how to use these domains to make the FMI resilient:

i. Governance
ii. Identification and Situational Awareness
iii. Protection
iv. Detection
v. Response and Recovery
vi. Testing



Thank you