ITUEvents

FIGI FINANCIAL INCLUSION GLOBAL INITIATIVE

FIGI Symposium

22-24 January 2019
Cairo, Egypt

#financialinclusion

Hosted by

NTRA National Telecom Regulatory Authority الجهاز القومي لتنظيم الإتصالات

Sponsored by

BILL & MELINDA GATES foundation

Organized by

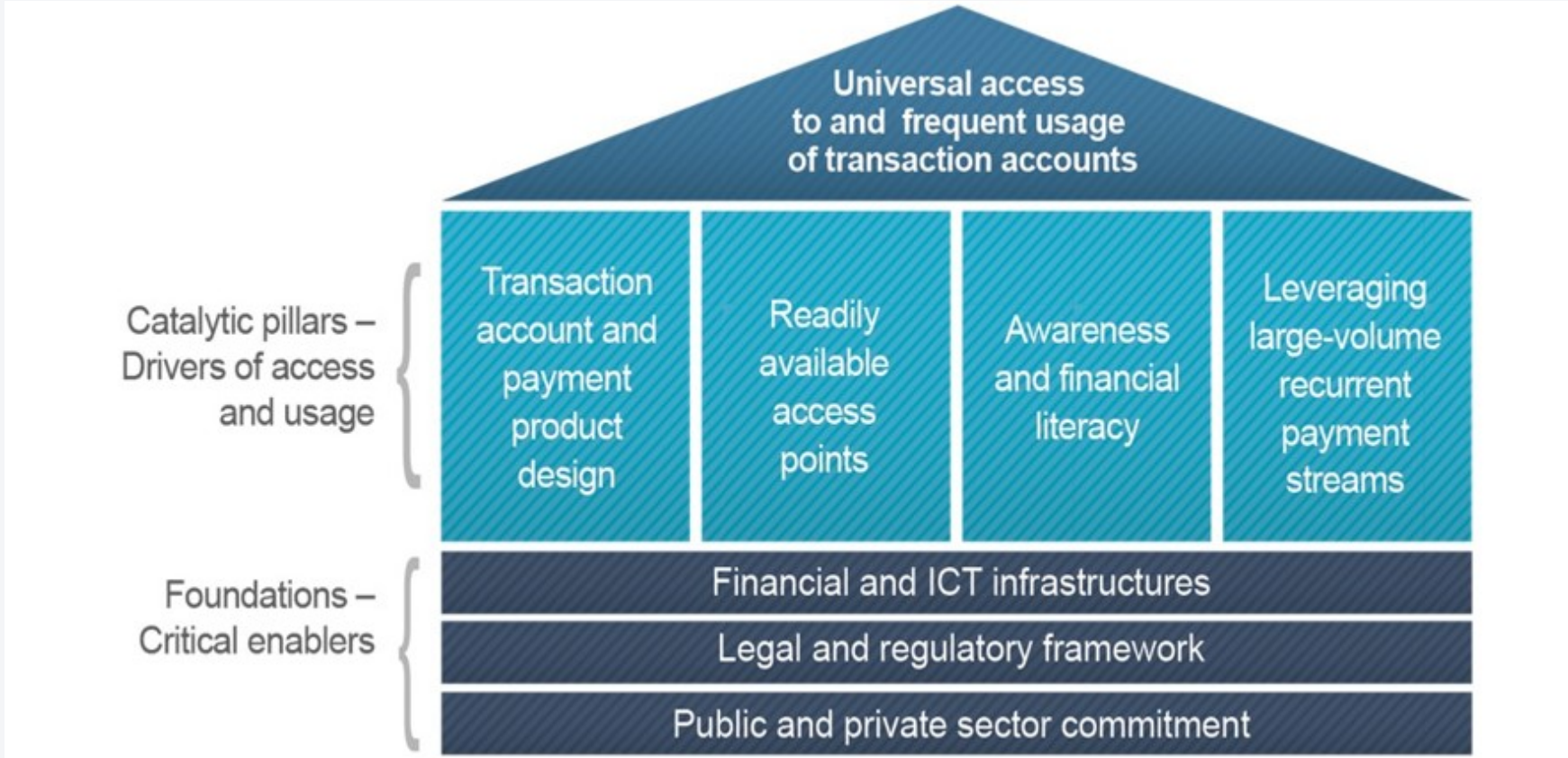
Committee on Payments and Market Infrastructures

BANK FOR INTERNATIONAL SETTLEMENTS

WORLD BANK GROUP

ITU

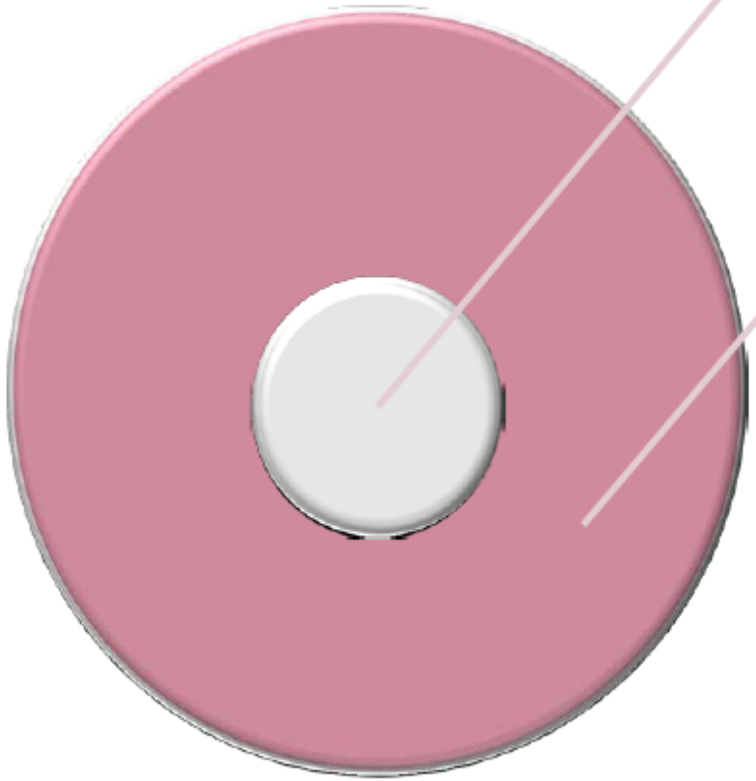
The CPMI-WB Payment Aspects of Financial Inclusion (PAFI) framework, 2012



FIGI FINANCIAL INCLUSION GLOBAL INITIATIVE

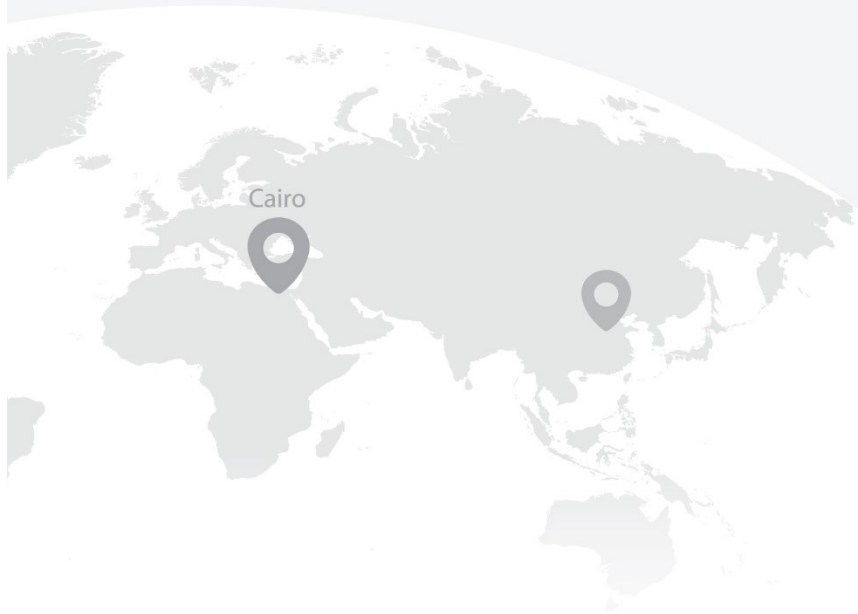
Broad strategy needed to address cyber resiliency, at various levels

FIGI FINANCIAL INCLUSION GLOBAL INITIATIVE



Protect the core

Secure the periphery



CPMI-IOSCO Guidance on cyber resilience for Financial Market Infrastructures (FMIs), 2016

FIGI FINANCIAL INCLUSION GLOBAL INITIATIVE

Eurosystem Cyber Resilience Strategy for FMIs

FIGI FINANCIAL INCLUSION GLOBAL INITIATIVE

1. FMI Readiness

- *Overseers should work with FMIs to enhance their cyber posture to ensure their safety and soundness against an increasingly sophisticated threat landscape*

2. Sector Resilience

- *Enhance and mature the collective cyber resilience capability of the Eurosystem financial sector, through cross-border/cross-authority collaboration , information sharing and exercisesC*

3. Strategic Regulator-Industry engagement

- *Develop a joint strategic and Board level pan-European FMI Regulator-Industry forum to establish trust and collaboration amongst participants, to catalyse joint initiatives to enhance sector capabilities and capacities, and increase cyber awareness.*

Tools: Cyber survey, European Red Team Testing Framework (TIBER-EU), **Cyber Resilience Oversight Expectations (CROE)**

Tools: market wide cyber exercises, info-sharing network, sector-mapping

Tools: Establishment of the Euro Cyber Resilience Board for pan-European FMIs (ECRB)

CROE – why?

- Sets up a more detailed elaboration of the **CPMI-IOSCO Cyber Guidance** to aid FMIs and overseers in operationalising 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 cyber maturity;
- Can be used as:
    a) **Assessment Methodology** for overseers; and
    b) Tool for **self-assessments for FMIs**.

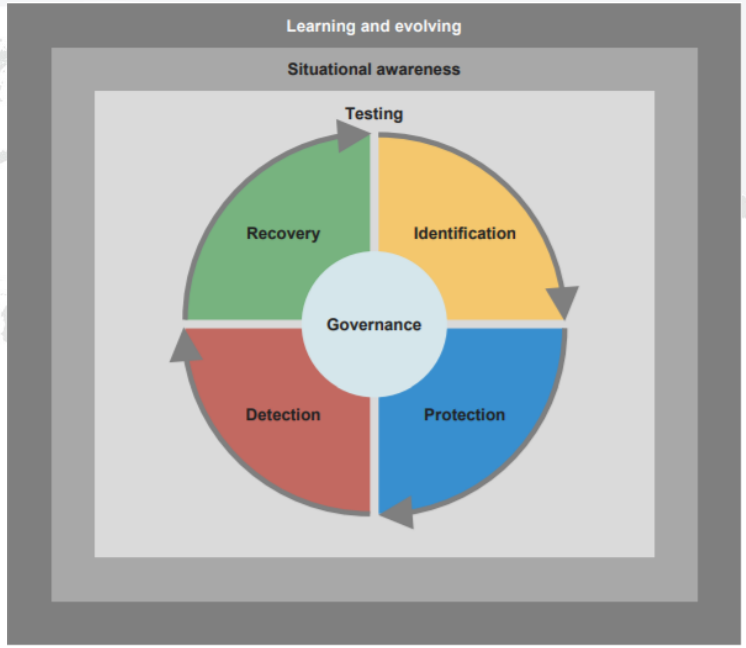
Main contents of the CROE

- **Addressees**
  - FMIs (mainly payment systems) operating in the Euro area and T2S
  - Euro area central banks may opt to use the CROE also for SSSs/CSDs and CCPs (in line with the applicable laws and regulations)

- **Structure**
  - The CROE is divided into 8 Chapters:
    - ✓ risk management: (i) governance; (ii) identification; (iii) protection; (iv) detection; and (v) response and recovery.
    - ✓ overarching components: (vi) testing;

      (vii) situational awareness; and

      (viii) learning and evolving.



High level messages from public consultation

- Overall, CROE positively received as a very useful set of practices for FMIs to apply.

- CROE should be harmonised with other international frameworks, as much as possible.

- The ECB should approach other key regulators, institutions and authorities(e.g. World Bank) to agree and standardize on a common framework, i.e. reduce the fragmentation of regulatory requirements, facilitate supervisory convergence and reduce the burden of additional cost on FMIs.

- CROE is comprehensive, but at times the controls are too prescriptive. The level of prescriptiveness may diverge from the regulatory harmonization efforts among regulatory and supervisory agencies and FMIs.

High level messages from public consultation

- There should be clarification on how FMIs will be expected to demonstrate compliance and how they will be assessed

- Request for a harmonised approach to assess FMIs between multiple regulators, especially for FMIs that are subject to oversight or supervision by several regulators. European CSDs, for example, are governed by multiple overseers and thus confronted with a fragmented regulatory landscape.

Changes in the CROE

- All comments have been reviewed and the CROE has been updated accordingly.

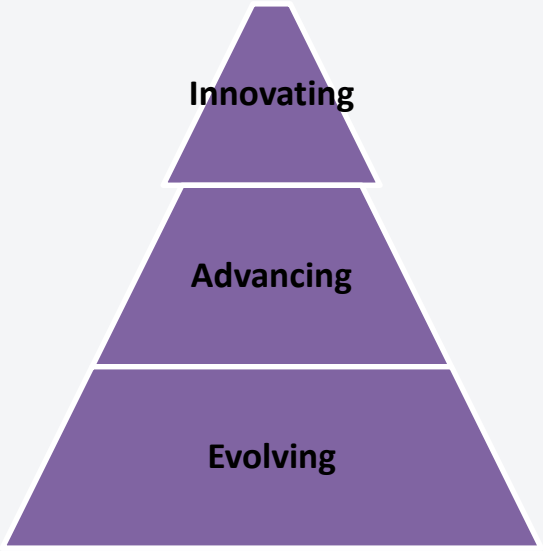
- "**Meet or explain**" approach has been adopted to allow a degree of flexibility for FMIs. FMIs may achieve the objective set out in the expectation, even if they use other controls (that are not cited in the CROE) to do so.

- The introduction will clarify the use of the maturity model – these are **levels of expectations** for overseers, not a replacement for existing international maturity models.

- Final CROE was published by the ECB in December 2018 and is now applicable to payment systems in euro area

Levels of expectations

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



SIPS/T2S

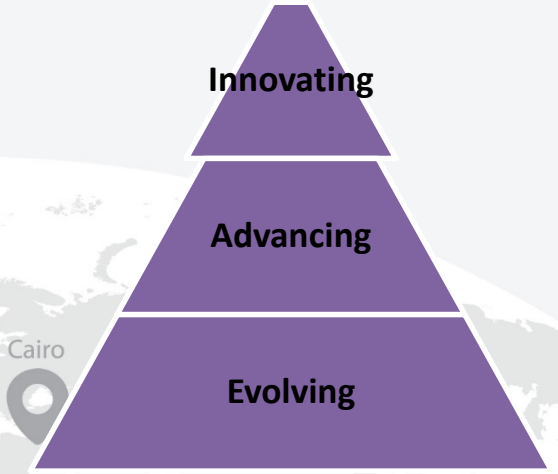
PIRPS/ORPS

- 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 - description

- **Evolving level:** *Essential capabilities* are:
  - established and evolve;
  - applied constantly across the FMI to identify and mitigate cyber risks, and
  - monitored and managed.

- **Advancing level:** meet the Evolving level, PLUS practices that:
  - incorporate more advanced implementations;
  - are integrated across the FMI's business lines, and
  - have been improved over time, to proactively manage cyber risks.



- **Innovating level:** In addition to meeting the Evolving and Advancing levels, this level entails:
  - driving innovation in people, processes, and technology for the FMI and the wider ecosystem to manage cyber risks and enhance cyber resilience
  - developing new controls, new tools, or creating new information-sharing groups.

Assessment process (under review)

- The operator writes a self-assessment up to the required level of expectation.
- If the expectation is „advancing“ the self-assessment must cover all elements in „evolving“ and „advancing“
  - An FMI can – if it wants to – also write a self-assessment for the level beyond the expected level;
  - An FMI can use the meet or explain principle if it does not meet an expectation, but feels that it achieves the intended outcome through another means;
- Operator submits self-assessment including background documentation
- Overseers assesse the materials:
  - Does the FMI meet the expectations?
  - If not, is the explanation provided sufficient?
- Overseer/operator meetings are held to discuss the material and agree on action plans to improve the system (if required)
- The overseer drafts a short CROE report which includes the weaknesses identified and recommendations for improvements
- The report is shared with the operator

CYBERSECURITY QUESTIONNAIRE: OBJECTIVE

FIGI FINANCIAL INCLUSION GLOBAL INITIATIVE

- Allows to understand the level of resilience of FMIs based on Different Levels of Expectations
- Allows financial sector authorities to benchmark best practices against peer economies
- Informs country diagnostic work
- Facilitate research into effectiveness of various policy reform approaches

Follow-up work

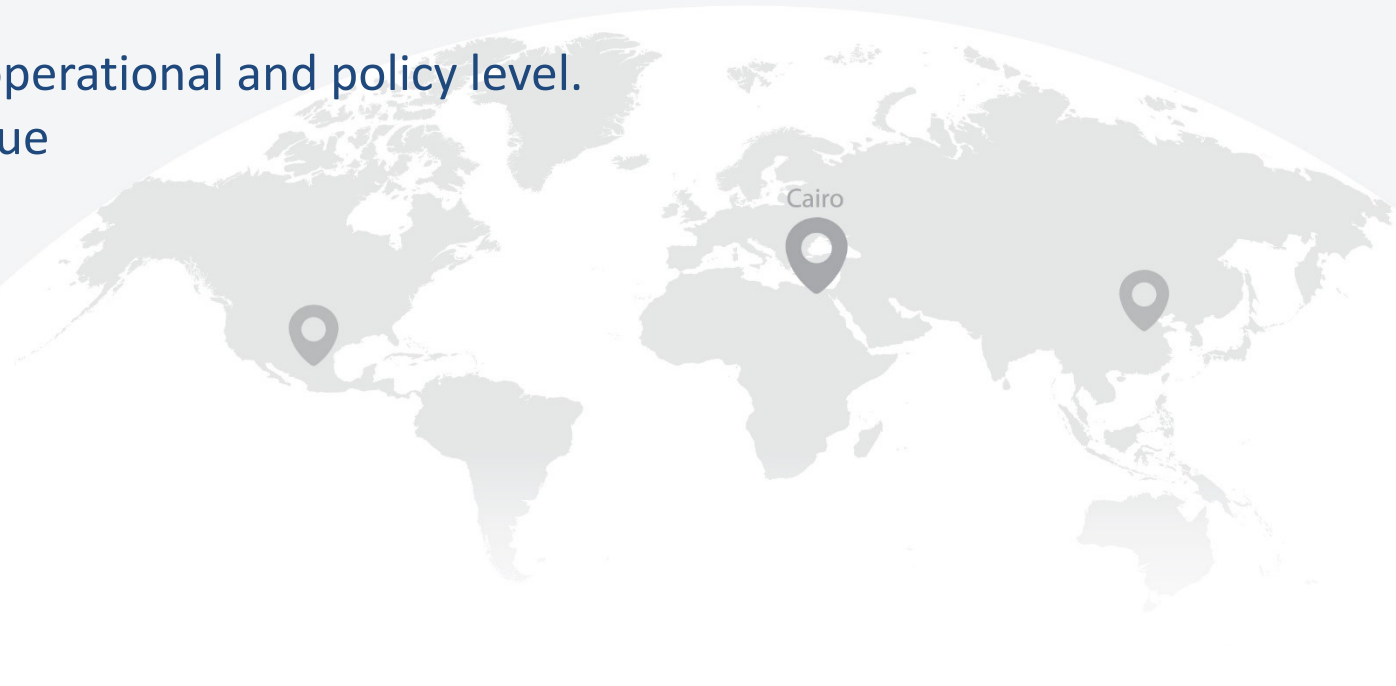
- **Information sharing:** newsletter and compendium

- **Step-by-step guide on how to build a cyber strategy for FMIs**

- **Testing**: FMIs are required to undertake different forms of testing. Need for an harmonized approach, applicable and useable for any type of entity.

- **Collaboration and cooperation** is essential at operational and policy level. Regulator – industry engagement: cyber dialogue

- **Dissemination and outreach**



FIGI FINANCIAL INCLUSION GLOBAL INITIATIVE

Thank you!