Update on international work on payments and financial markets infrastructures *

Ninth Conference on

Payment and Securities Settlement Systems

Ohrid, 6 June 2016

Klaus Löber

* Views expressed are those of the author only

The Committee on Payments and Market Infrastructures

Mandate

⇒ To promote the safety and efficiency of payment, clearing, settlement and related arrangements, thereby supporting financial stability and the wider economy, and to monitor and analyse developments in these arrangements, both within and across jurisdictions

- Establishment in 1990 as *Committee on Payments and Settlement Systems* (until 1 September 2014); preceded in 1980 by the G10 *Group of Experts on Payment Systems* and the 1989 ad hoc *Committee on Interbank Netting Schemes*
- Chaired by Benoît Coeuré (ECB); hosted by the Bank for International Settlements in Basel), reporting to the Governors of the Global Economy Meeting
- Enlarged in 1997-1998 and then in 2009, so that it now includes 25 central banks

The Committee on Payments and Market Infrastructures

Tasks

⇒ The CPMI is a global ***standard setting body*** in the field of payments, clearing and settlement systems and related activities (also including the formulation of common policies and recommendations):

e.g. *Central bank oversight of payment and settlement systems* (2005)

Principles for financial market infrastructures (2012)

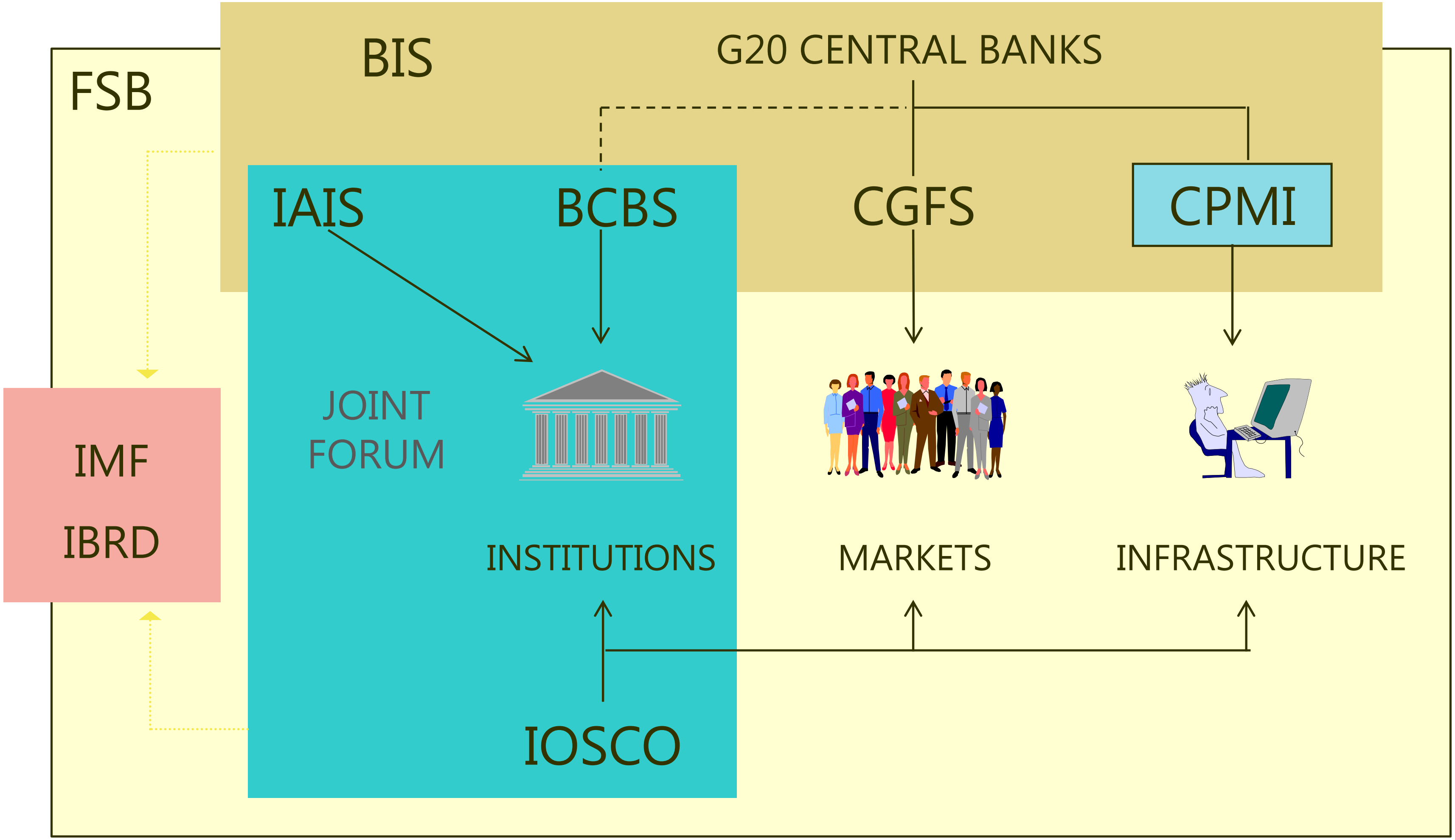
⇒ It also serves as a ***forum for central banks*** to *monitor and analyse developments* in large value and retail payment, clearing, settlement and related arrangements, schemes and instruments, both within and across jurisdictions (also including cooperation and sharing information, increasing common understanding, etc.):

e.g. *Role of central bank money in payment systems* (2003)

The interdependencies of payment and settlement systems (2008)

Innovations in retail payments (2012)

The "Basel process" (simplified)



Evolution of CPMI activities

Herstatt

G10 Group of Experts on Payment Systems

G10 Ad hoc Committee on Interbank Netting Schemes (Lamfalussy)

CPSS

(Allsopp) Report on Settlement Risks in FX

E-money

Core Principles for SIPS

Recommen-dations for SSSs (w IOSCO)

CLS

Recommen-dations for CCPs (w IOSCO)

Report on Oversight

General principles on remittances (w World Bank)

Interdepen-dencies

FX settle-ment risk

Lehman

Principles for FMIs

Virtual currencies

Retail payments

Correspon-dent banking

OTC derivatives data harmonisation (w IOSCO, FSB)

FMI recovery and resolution (w IOSCO, FSB)

Cyber resilience

Role of non-banks

Digital innovations

1974 1980 1989 1990 1991 1992 1996 1999 2001 2002 2003 2004 2005 2007 2008 2009 2012 2014 2015

Top CPMI priorities

- Implementing the Principles for Financial Markets Infrastructures (FMIs)
- FMI resilience (incl. cyber resilience), recovery and resolution
- Payment developments
- Digital innovations
- Evolution of oversight approach and cooperative arrangements

Evolution of central bank oversight

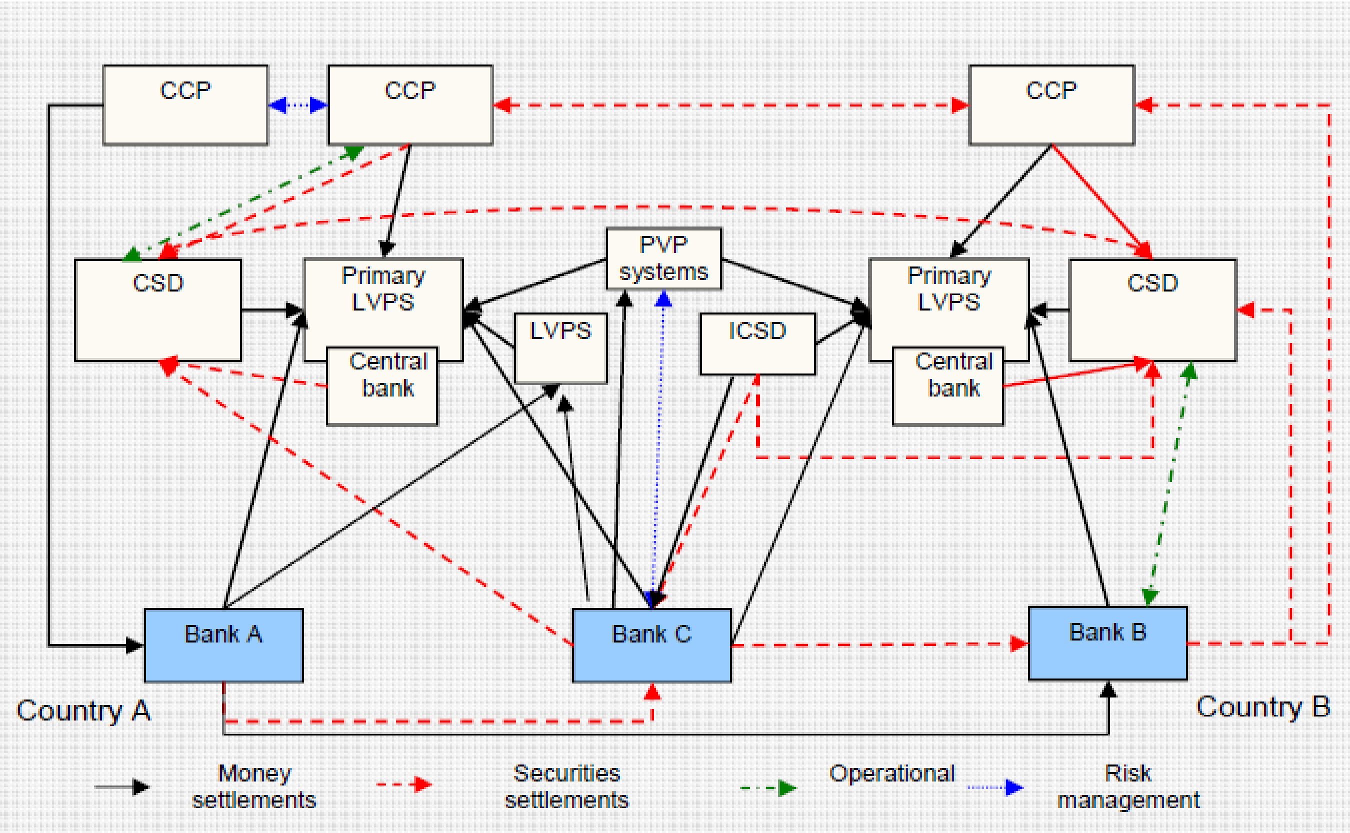
Oversight of [payment and settlement] [systems] is a central bank function whereby the objectives of safety and efficiency are promoted by monitoring existing and planned systems, assessing them against these objectives and, where necessary, inducing change

Central bank oversight of payment and settlement systems, May 2005

- Oversight of what? – Systems? FMIs? Arrangements? Others?
- Oversight by whom? – Central banks? Other authorities?
- Oversight what for? – Safety and efficiency
- Oversight how? – Monitoring, assessing, inducing change

Increasing complexity

- *Interdependencies*
  - Links
  - Tiering
- *Cross-border*
  - services
  - participation
- Non-banks
- Quasi-systems



Multiple authorities:

- Central Banks
- Financial stability bodies
- …
- Market regulators
- Competition authorities
- Bank supervisors
- Resolution authorities

⇒ *also cross-border*

The PFMIs "ecosystem"

Implementation monitoring

Assessment methodology (2012)

Disclosure framework (2012)

Add. quantitative disclosures (2015)

Recovery and resolution (2014, …)

PFMIs (2012)

24 Principles +
5 Responsibilities

Application of PFMIs to central bank FMIs (2015)

Stress testing, fin. resources, gover-nance (mid 2016)

Critical service providers (2014)

Recommendations for settlement (forthcoming)

Further guidance (tbd)

Reporting, data harmonization (LEI, UPI, UTI) (2015,…)

Collateral management services (2014)

Repos and sec. lending (2010,…)

Cyber resilience (2014, 2015,…)

Status of CPMI standards

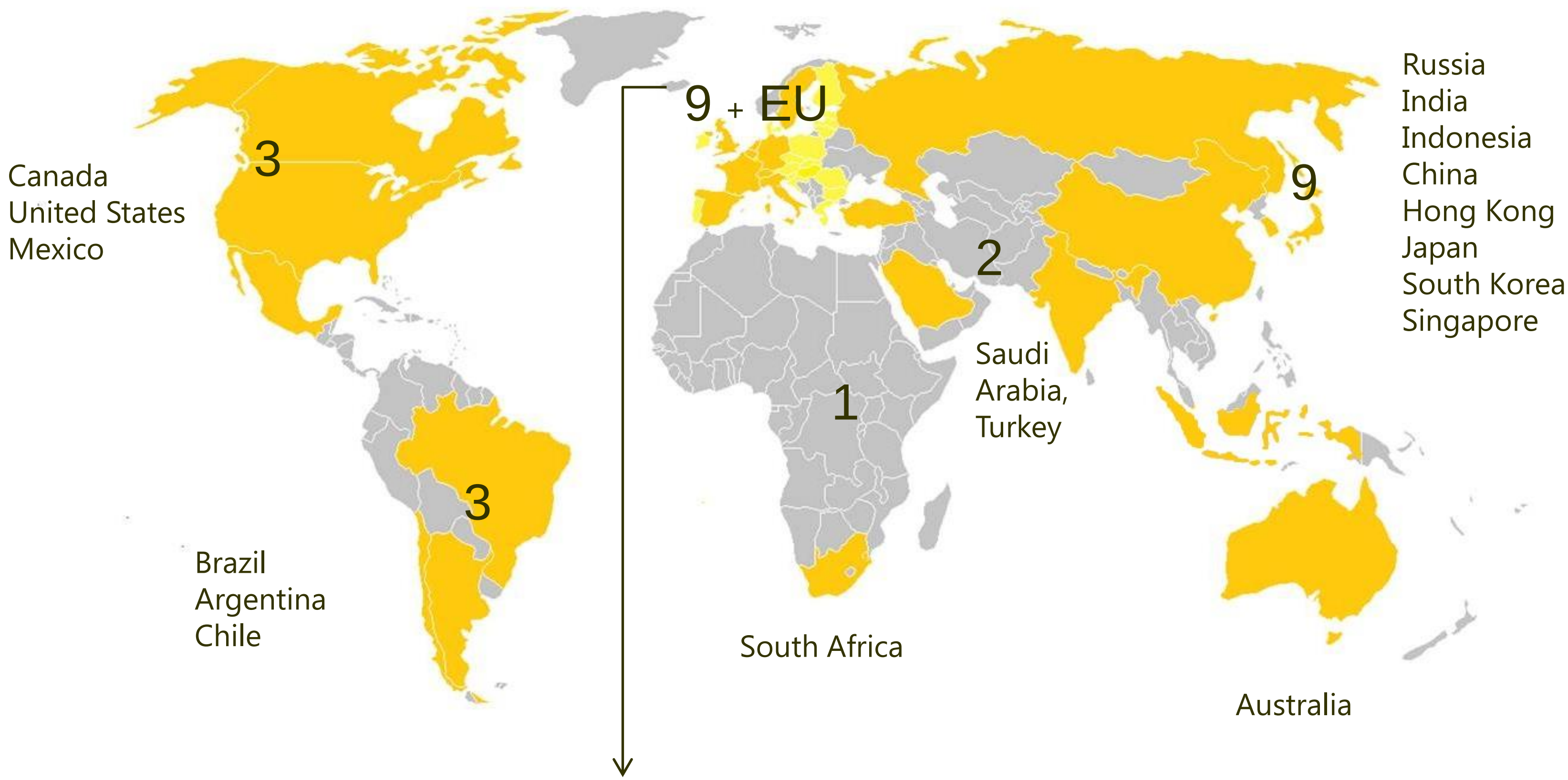
- *Not legally binding* as such but national regulation increasingly based on them (sometimes by way of incorporation) because of:
  - Power of the arguments they contain ("*soft law*")
  - *Commitment of members* of the relevant bodies
  - Compliance of CCPs with the PFMIs is a condition for banks to benefit from lower capital requirements
- Subject to *implementation monitoring* by CPMI-IOSCO (and FSB monitoring, IMF and World Bank FSAPs)
  - Implementation may be rules-based, principles-based or a combination of both
  - Focus on consistency of outcomes at the level of FMIs across jurisdictions

PFMI implementation monitoring

- *Full, timely and consistent implementation of the PFMIs* is fundamental to ensuring the safety, soundness and efficiency of key FMIs and for supporting the resilience of the global financial system
- *CPMI and IOSCO members are committed* to adopt the principles and responsibilities in line with G20 and FSB expectations
- In April 2013, CPMI and IOSCO *started the process* of monitoring implementation of the PFMIs
- Reviews are carried out in ***three stages***:
  - Level 1 - ensuring the *timely* implementation
  - Level 2 - ensuring *regulatory consistency*
  - Level 3 - ensuring consistency of *outcomes* *(across FMIs and across jurisdictions)*

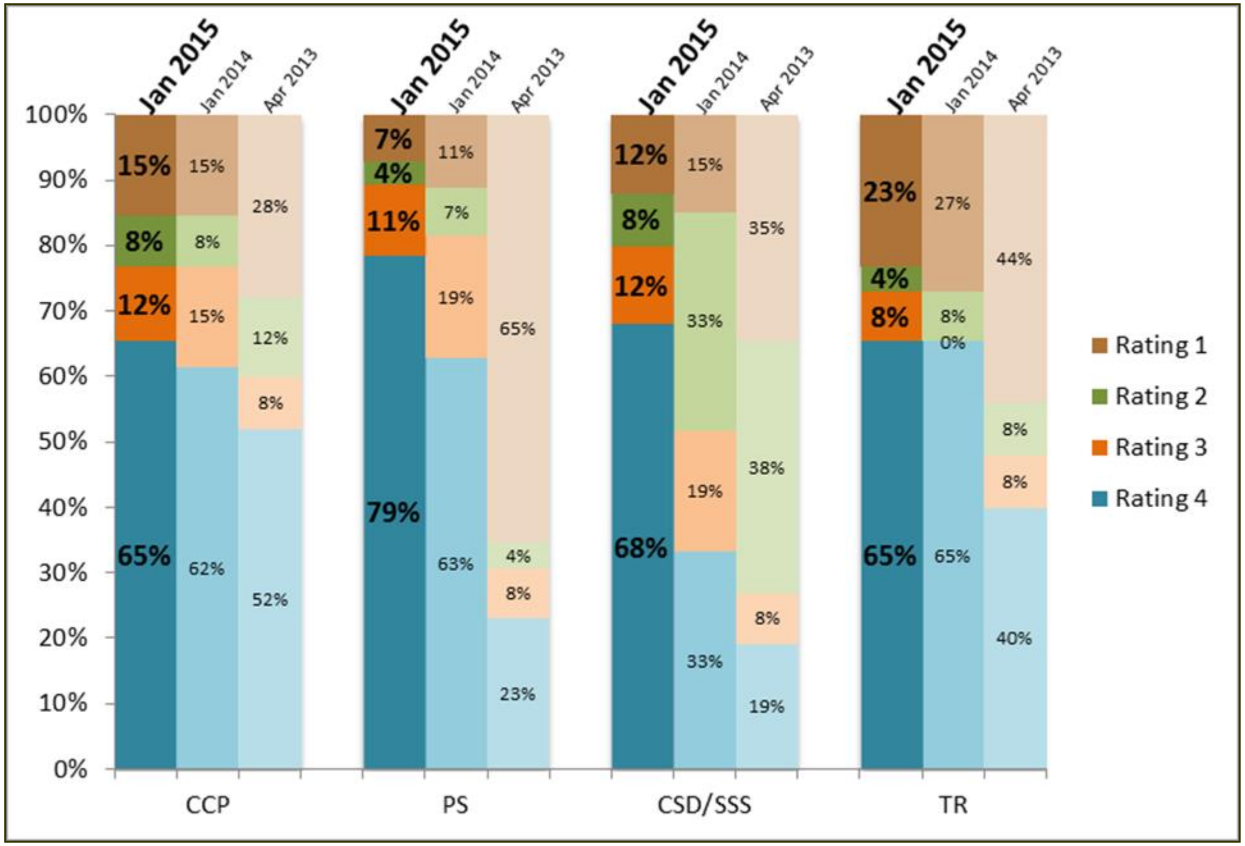
Implementation monitoring - Scope

- Geographical coverage: Commitment of members of the relevant bodies (CPMI, IOSCO, FSB) to adopt the PFMIs



EU, Belgium, Netherlands, France, Italy, Spain, Germany, Switzerland, UK, Sweden

Level 1 Update 2: Progress for Principles by FMI type



Need for new or more stringent standards for FMIs?

FMIs are subject to ***comprehensive international standards***, the CPMI-IOSCO *Principles for financial market infrastructures* (PFMI), issued in 2012 and subsequent ***complementary guidance*** (e.g. on *disclosures, recovery, cyber resilience*)

- ***Are the standards being observed?***
  - Lags in adopting and enforcing the standards
  - Differences in interpreting the standards

  ⇒ *Time, peer pressure/monitoring and more guidance*

- ***Are the standards enough? Are they effective?***

  ⇒ *Implementation monitoring, market-wide stock-take and analysis of the effects of the measures taken to see if systemic risk has been reduced enough*

Resilience, recovery and resolution of FMIs

- CPMI-IOSCO guidance on ***FMI recovery***
- FSB Key attributes for the ***resolution*** of SIFIs – ***FMI annex***

⇒ Need for continued provision of *critical infrastructure services* to markets

⇒ *Continuum* of FMI risk management, recovery, resolution

⇒ Clear and transparent *determination of tools and loss allocation rules*

⇒ *Recovery and resolution planning* by FMIs and authorities

⇒ *Interest of FMI participants* (including their clients and supervisors)

Follow-up work

- FMI ***resilience*** (CPMI-IOSCO)
  - Assess CCP *governance, financial resources and stress-testing models*
  - Additional focus on *cyber resilience*
  - Assess need for further *transparency/disclosure* requirements

  ⇒ Possibility of additional guidance or more granular standards
- FMI ***recovery*** (CPMI-IOSCO, with FSB)
  - Assess the current status of CCP recovery planning

  ⇒ Possibility of more granular standards
- FMI ***resolution*** (FSB, with CPMI-IOSCO)
  - Stocktake of CCP resolution regimes and resolution planning
  - Assess the need for additional capital and liquidity resources in resolution

  ⇒ Minimum standards for resolution planning (building on *Key Attributes*)
- Plus: FMI/participant ***interdependencies*** and ***cooperation of authorities*** (BCBS, CPMI, IOSCO, FSB)

Global TR aggregation and Global Identifiers

- Need to establish *centralised or other mechanisms* to produce and share *global aggregated data* that authorities need to fulfil their mandates and to monitor financial stability (work conducted by FSB jointly with CPMI and IOSCO)
  - legal constraints (secrecy and confidentiality rules)
  - technical issues (standardisation and harmonisation of data)
- Global *Legal Entity Identifier* (LEI) System
  - A global scheme for the issuance of legal entity identifiers that will *uniquely identify parties to financial transactions*
  - The *Regulatory Oversight Committee* (ROC) was established in January 2013 - CPMI is a member of the Executive Committee of the ROC
- Further work by CPMI and IOSCO on *Unique Product and Transaction Identifiers* is on-going

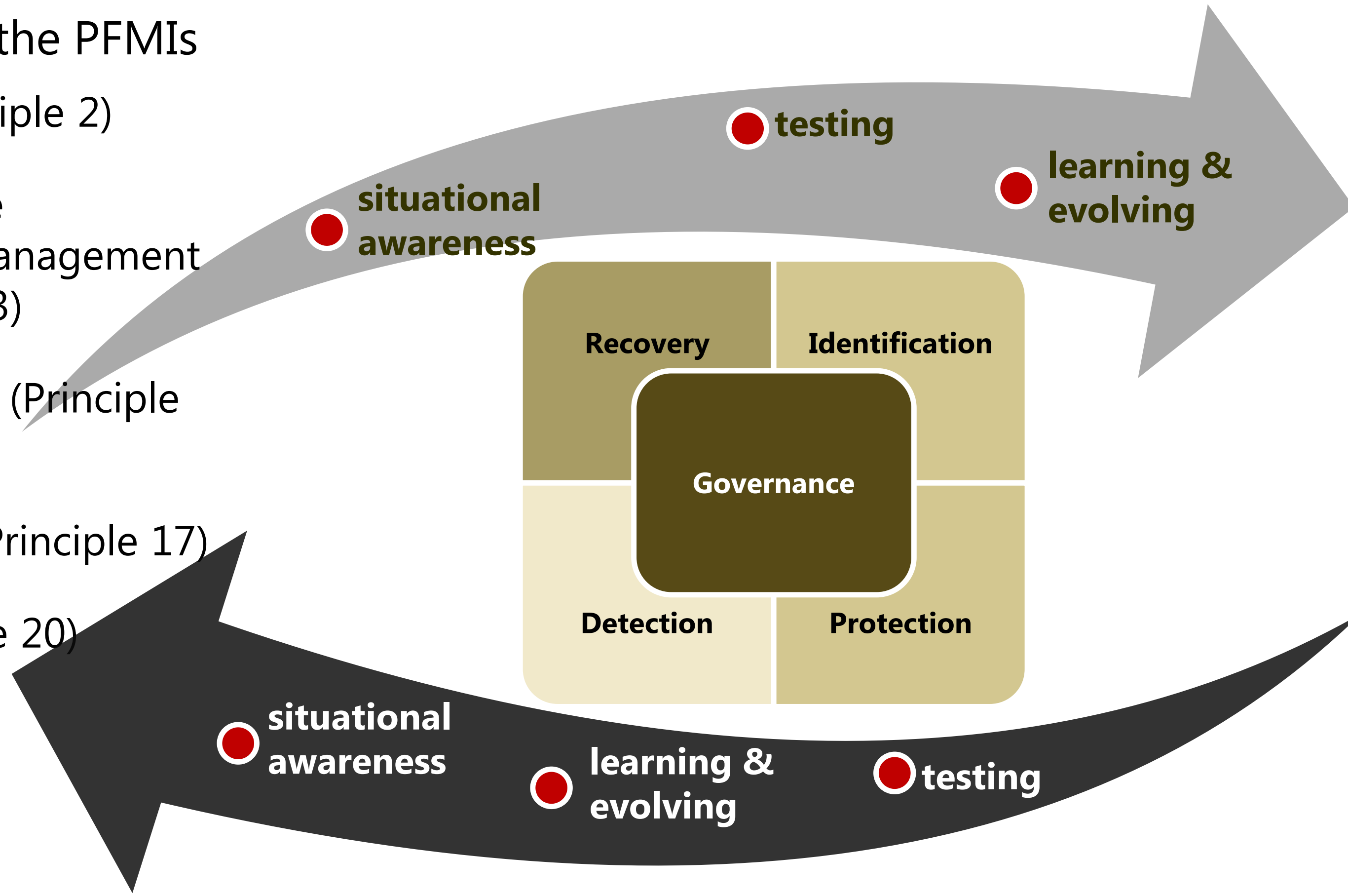
CPMI work on cyber resilience of FMIs

- In 2012 , set up of a CPMI working group to analyse cyber security issues, including epresentatives from IOSCO and BCBS
- **CPMI report** published in November 2014 - Key findings:
  - Diversity of goals (cyber-activism, fraud, terrorism, etc.)
  - Increasing sophistication of attacks - multiplicity of entry points
  - Disruption can entail comprehensive data/system integrity breach
  - Diversity of measures needed (IT, processes, people, communication) – focus on worst case scenarios and potential quick recovery mechanisms

- In 2014, CPMI and IOSCO set up a joint WG on cyber resilience (including BCBS and IAIS representatives) working on **further guidance**

Guidance on FMI cyber resilience

- Supplemental to the PFMIs
  - Governance (Principle 2)
  - Framework for the comprehensive management of risks (Principle 3)
  - Settlement finality (Principle 8)
  - Operational risk (Principle 17)
  - FMI links (Principle 20)
- Principle-based



⇒ Actions across these guidance categories can be mutually reinforcing and should be considered jointly in order to achieve resilience objectives

Key findings for FMI cyber resilience

- **Board and senior management** attention is critical to a successful cyber resilience strategy
- The ability to **resume operations quickly and safely** after a successful cyber attack is paramount
- FMIs should make use of good quality **threat intelligence and rigorous testing**
- Cyber resilience requires a process of **continuous improvements**
- Cyber resilience cannot be achieved by an FMI alone; it is a **collective endeavour** of the whole ‘eco-system’

⇒ **Data integrity** - growing awareness that it needs to be addressed by FMIs and the industry as a whole - Thus, cyber resilience should **not a point of competition** among FMIs

⇒ FMIs and overseers are convinced that more needs to be done in terms of **cooperation and information sharing** – the financial system is as strong as its weakest link in a world of **interconnectedness and interdependencies**

Outlook

- Comprehensive **global regulatory standards** form the basis for adequate national regulation, supervision and oversight mitigating systemic risks

- Global **regulatory convergence and coordination** is an indispensable pre-condition to achieve consistency of results and to avoid cross-border distortions

- Enhancing the **cooperation of authorities** and ensuring the **sharing of information** as needed to fulfil authorities‘ mandates is a pre-condition to foster financial stability

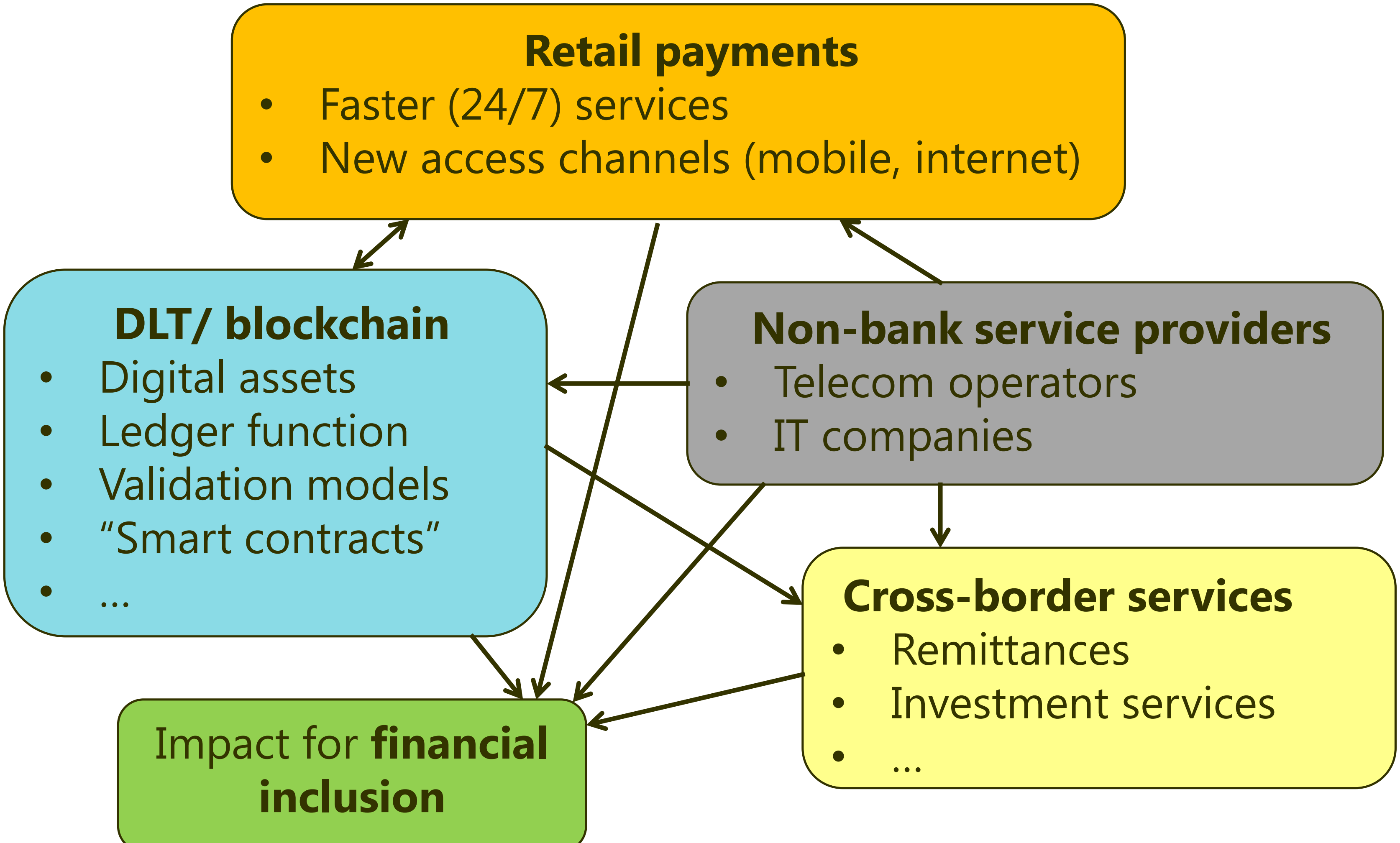
⇒ ***Need for a continued further review of the global regulatory architecture***

Innovations in payments

- *Dynamic market*, but few innovations have significant impact (so far), regional differences are likely to persist
- *Speed* is gaining importance in payments (real-time)
- *Blockchain, DLT* facilitate global peer-to-peer transfers
- *Role of non-banks* is increasing
- *Security issues* will become ever more critical
- Role of *standardisation*?
- *Financial inclusion* is a driving force

⇒ *Regulation can be either driver or barrier*

Innovations



CPMI Working Group on Retail Payments

- **Mandate**
  - Look at recent developments in the field of retail payments,
  - Identify those that have the highest potential to affect the wider payment ecosystem, and
  - Analyse potential implications and emerging risks, with a particular emphasis on the implications for central bank functions and policies
- Areas of interest identified:
  - **Fast and continuously available retail payment services** (inc. an interplay of these services with mobile/internet payments)
  - **Digital currencies** (report published in 2015)
  - **Cross-border retail payments**

Fast payments

- Concept of “fast payments” may not be as clear as it sounds

- Speed and continuous service availability are key features, but there are other features that are usually implicit, but necessary

Fast payments

- Increasingly gaining the **attention of central banks** as they are quickly changing the retail payments landscape and bringing about operational and financial issues that need to be managed
  - Dramatically enhancing the *speed and availability of retail payments*
  - Central banks are *backing or leading initiatives* for the implementation or even providing *operational support* (eg enhancing RTGS systems)
- Areas for further **analysis**:
  - *Definition and classification* of fast payments
  - *Drivers and barriers* to the development of fast payments
  - Implications of fast payments for *efficiency and risk*, and
  - Issues particularly relevant to *central banks*

CPMI working group on digital innovations

- Disruptive innovations in can have important implications for payments, trading, clearing and settlement, and thus are monitored by relevant authorities in their ***oversight capacity***
- Innovations based on electronic and IT schemes have been analysed since the mid-90ies (see eg CPSS e-money reports)
- ***Blockchain*** and ***distributed ledgers*** are innovations that can ***potentially disrupt*** many areas of the financial industry
- As part of the shift in focus towards new and disruptive innovations, the emergence of ***digital currencies frontrunning developments in other field*** (already noted in recent reports by the CPMI on ***innovations*** (2012) the role of ***non-banks in retail payments*** (2014), and on ***digital currencies*** (2015)

⇒ **CPMI working group on digital innovations** set up in 2015

⇒ Joint work with IOSCO and other committees under way

Digital currencies and blockchain

- There are two key features of digital currencies:
  - the ***assets*** themselves (typically not a liability of any entity nor backed by a public authority) - currently, such schemes are *not widely used or accepted* and their *likely impact is limited*
  - the ***technology*** used, in particular the use of *distributed ledgers*, allowing transactions in the absence of trust between the parties and without the need for intermediaries
- Current schemes ***evolve very quickly***, but a pattern seems to be emerging with the increasing *use of the underlying technology*
- Blockchain solves a fundamental glitch of previous generations of digital schemes: it prevents digital assets from being *re-used* (***double spending problem***) and deals with the ***absence of trust***
- Even if current schemes do not persist, the underlying technology may have the ***potential to improve the efficiency of financial services and enhance financial inclusion***

Implications of blockchain / distributed ledgers

- If widely used, a ***challenge the intermediation role*** of current actors in the financial system (FMIs, banks, brokers, remittances)
- ***Potential to induce changes*** in
  - trading (exchange function)
  - transfers (payment, clearing and settlement services) and
  - holding of assets (records of ownership)
- Specific ***issues of relevance***:
  - permissionless vs restricted models (access and governance)
  - validation (involvement of users or not)
  - database/ledger function (eg consensus based ledgers)
  - “smart” contracts (conditionality elements, automatism)
- This might lead to changes in the way the financial system works – ***business models*** *(**competition vs. cooperation**)*, **centralisation**, ***risk management, supervision***

Risks

- **Legal risk –** no legal certainty or clarity on the nature of the asset and on the rights and obligations of the parties to a transaction
- **Consumer protection and risk of theft** - digital services are not well understood by consumers (but not only by them), who may therefore not appreciate the risks involved; most digital assets are relatively anonymous and are typically stored in digital wallets, which can be hacked and the units of value could be stolen
- **Operational risk** - the decentralised setup of a blockchain and its open and governance structure make it open to hacking attacks on exchange platforms or changes of the underlying protocol
- **Anti-money laundering and terrorist financing** – no central entity is responsible for performing KYC duties; the best proxy being access points (e.g. digital currency exchanges or wallet provider)

Involvement of regulatory standard-setting bodies

- ***Sectoral and cross-sectoral analysis and evaluation***
  - monitoring ***developments and evolution*** of digital schemes
  - ***technical aspects*** of blockchain and impact on services and systems
  - ***legal aspects*** (legal classification, rights and obligations of issuers and service providers, client asset protection)
  - ***security***, scalability and ***operational (cyber) resilience*** of financial products and services based on blockchain
  - relevance for ***AML / TF***
  - impact on ***financial intermediation*** and role of financial institutions
  - relevance for ***financial inclusion***
  - wider impact on ***financial stability***
- ***Assessment of need for global regulatory guidance*** (risk-based approach)

Cross-border payments

- Although there have been *new developments in cross-border payments*, there are concerns that the market as a whole is not well understood and significant barriers remain to further meet market demands
  - **Need to better understand** the landscape as well as the specific role of central banks and associated issues and challenges
- Potential areas for further **analysis**:
  - Furthering understanding on the cross-border payments landscape and the solutions currently available
  - Furthering understanding of *risk and efficiency* issues of concern to central banks and financial institutions, and
  - Examining the *role of central banks in cross border payments*

CPMI working group on correspondent banking

- CPMI working group to analyse the issue of correspondent banking from a **central bank's perspective** with a **focus on payment system implications**
- A **consultative report** was published in October 2015
- The report provides some basic definitions (incl. main types of correspondent banking arrangements), summarises recent developments and touches upon the underlying drivers
- The report puts forward **recommendations** concerning the development, promotion and use of four **technical measures**
  - if implemented in the payment process, these could reduce some of the **costs** associated with regulatory compliance
  - however, in isolation, these technical measures will not resolve all issues connected with correspondent banking activities, and
  - the technical measures will not as such help the banks without access to correspondent banking services to gain such access

Correspondent banking

Four technical recommendations:

- Use of *know-your-customer (KYC) utilities*
  (templates and procedures to identify the most appropriate data fields to compile a data set which)
- Increased use of the *Legal Entity Identifier (LEI)*, where possible
  (including promoting BIC to LEI mapping facilities)
- Use of *information-sharing initiatives* as an information source by default
  (where they exist and data privacy laws permitting; need for additional clarity on due diligence recommendations for upstream banks ("KYCC"))
- *Improvements in payment messages*
  (determination whether the Serial method using MT 103 or the Cover method using MT 103 and MT 202 COV is preferable)

Financial inclusion

- CPMI and World Bank *Joint task force on payments aspects of financial inclusion* (PAFI)
- ***Consultative report*** issued in September 2015
  - Examining demand and supply side factors affecting financial inclusion in the context of payment systems and services
  - Ideally, all individuals and businesses should have access to and be able to use at least one transaction account operated by a regulated payment service provider, to:
    (i) perform most, if not all, of their payment needs
    (ii) safely store some value; and
    (iii) serve as a gateway to other financial services

Financial inclusion

- Seven **guiding principles** designed to assist countries that want to advance financial inclusion in their markets through payments
  (i) *commitment* from public and private sector organisations
  (ii) a *robust legal and regulatory framework* underpinning financial inclusion
  (iii) safe, efficient and widely reachable financial and ICT *infrastructures*
  (iv) *transaction accounts* and payment product offerings that effectively meet a broad range of transaction needs
  (v) *availability* of a broad network of access points and interoperable access channels
  (vi) effective *financial literacy* efforts; and
  (vii) the *leveraging of large-volume and recurrent payment streams*, including remittances, to advance financial inclusion objectives

Outlook for the payments area

- Reaction of the incumbents (such as banks and traditional ACHs) on innovations and new competitors ("**second round**" **effects)**
- Impact of **digital innovations** (especially technical aspects)
- Promotion of **cyber resilience**
- Leveraging by relevant public bodies on **payments aspects of financial inclusion**
- Global **standardisation** (by standard-setters and industry bodies)
- Initiatives to enhance **(cross-border) interoperability**

⇒ ***Oversight frameworks*** to be adapted to the evolving landscape

⇒ Need for ***cooperation and coordination*** of central banks and other authorities (at the national and international level)