CEMLA
CENTRO DE ESTUDIOS MONETARIOS LATINOAMERICANOS

Cybersecurity: a perspective from LAC Central Banks

Financial Sector Cyber Resilience Workshop

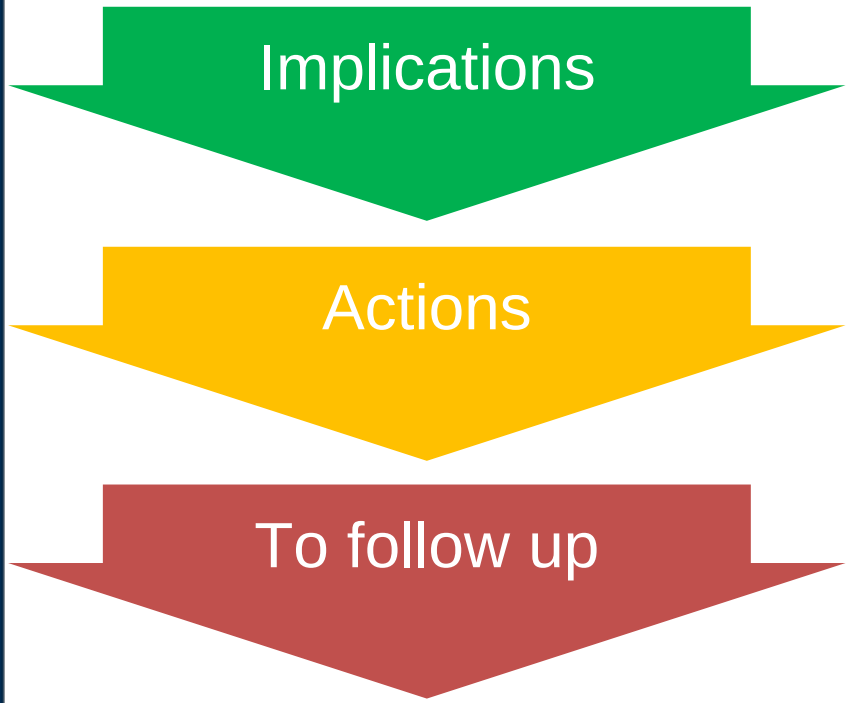
Raúl Morales and Gerardo Gage
CEMLA

6 November 2019, Mexico City

**Views expressed in this presentation do not reflect those of CEMLA or any of the Associate Members

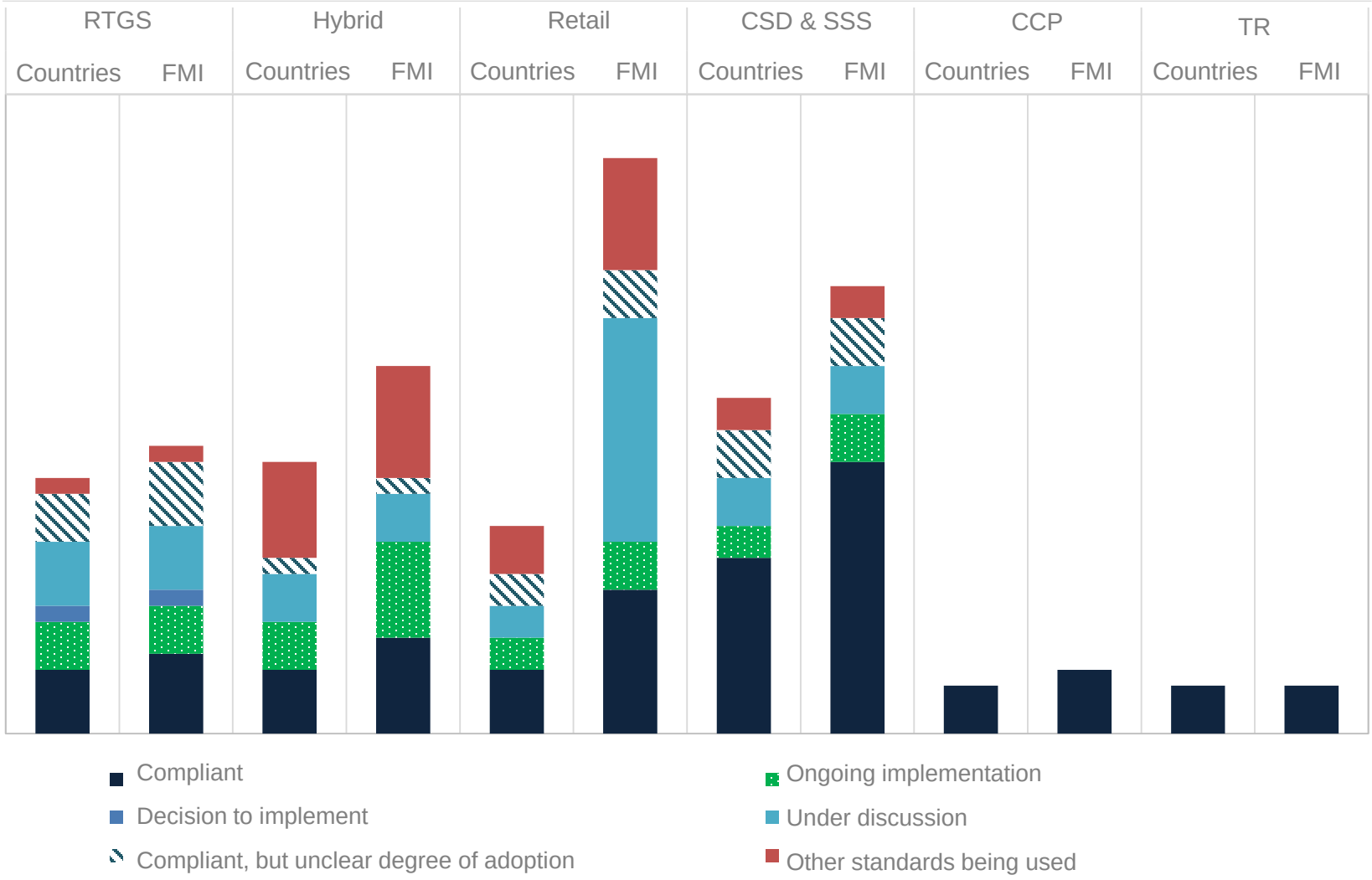
CPMI-IOSCO Principles (& Cyber Guidance)

- Objective: To determine the capacity of central banks for the implementation of the Principles in financial market infrastructures.



- Significant increase of requirements than the previous standards.
- Adoption required a comprehensive understanding of the ecosystem (PSP, interdependencies, etc.) and an impact assessment.
- Novelties related to access, operational (including cyber) and business risks.

Self assessment (2015-16)



Source: CEMLA (2017)

Issues related to Operational (inc. cyber) risk

IMPLICATIONS

- To adapt operational risk management mechanisms (backup site, guaranteeing critical services, RTO, regular tests against cyber threats).
- Compliance with Annex F (Expectations about critical service providers).
- Need for (greater) interinstitutional (formal) cooperation to avoid oversight gaps.

POTENTIAL ACTIONS

- To analyze the responsibilities of relevant authorities to detect inconsistencies, uncovered aspects or potential duplications.
- To assess suitability of cooperation agreements (existing or tacit).

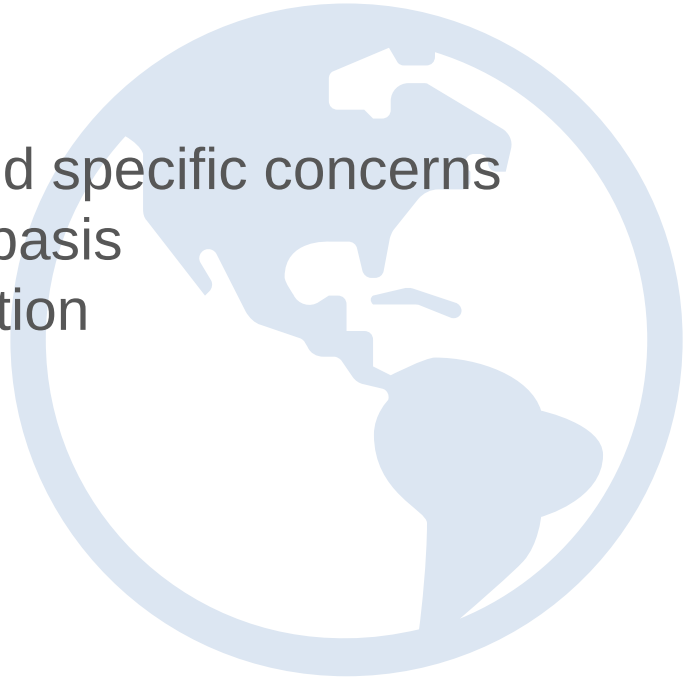
Issues related to Operational (inc. cyber) risk

To further address

- It would be convenient to establish a standardized process to verify compliance with recommendations on operational risk.
  - To overcome coordination challenge (beyond the individual efforts of each FMI).
- Measures to achieve formal cooperation mechanisms between authorities.
  - Role for common minimum criteria be established in aspects subject to discretion/interpretation.
- Authorities: powers, resources and coordination among them.
- Ensuring that appropriate rigor is applied in the entire ecosystem
  - Focus on organizational arrangements, including independent unit to be required (CISO)

Regional cooperation: FOCOSC

- Regional forum on cybersecurity, established in 2016
  - 15 national central banks, +50 users
  - Regular remote meetings
- Platform to exchange news and specific concerns
  - Participation on a voluntary basis
  - Ad-hoc exchange of information



2019 Regional survey on cyber security practices

- 12 Central banks
  - 9 Latin American, 3 Caribbean
- 100% of them are:
  - Developing (or already have) its current cybersecurity strategy/framework, following international standards.
  - Implementing monitoring tools for cyber threats detection.
  - Agreed with the CPMI definition on cyber risk.
- None of them:
  - Have an insurance plan for cyber issues.

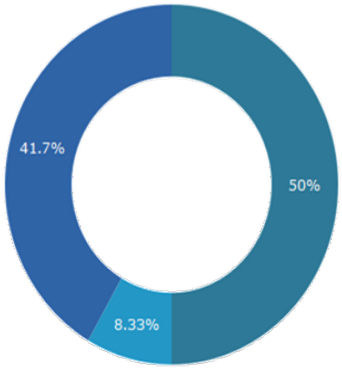
CEMLA
CENTRO DE ESTUDIOS MONETARIOS LATINOAMERICANOS

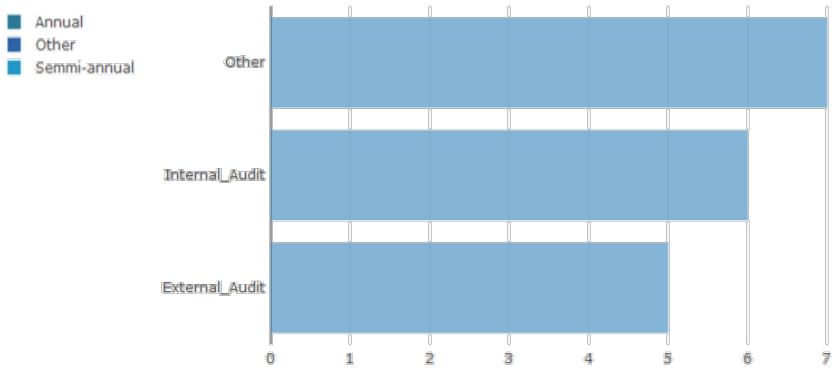
Governance

- 10/12 central banks have an area/division responsible for cybersecurity issues.
  - 2/3 central banks rely on the existing regulatory framework to supervise cyber risk.
  - Less than 50% have identified (or have) a policy for resources and tools to advance their cybersecurity framework
- Besides a specific area in charge, 3/4 central banks have a committee overseeing cyber security objectives across the institution
  - Including IT, Payments, HR and other core areas.
  - Appointed by the Board.
  - Besides monitoring, the committee advises and establishes guidelines on cyber and information security.

Risks identification

- All jurisdictions reported a risk-based approach to identify critical information, functions and processes.
  - Controls are defined against this approach and reviewed on a regular basis (mostly, annually), but in 50% of cases, there is no formal review process. (left chart)
  - In most cases, the review is double eyed, internal plus external audit. (right chart)
- Only 2/12 has a cybersecurity strategy and framework that distinguishes between entities types.
  - Proportionality is an aspect that could be useful to ensure appropriate and reasonable controls are implemented.
  - Information and services may be critical or not, depending on the type of entity.





CEMLA
CENTRO DE ESTUDIOS MONETARIOS LATINOAMERICANOS

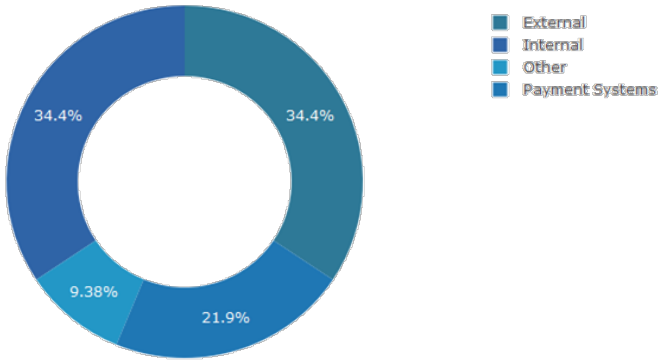
Protection

- LAC central banks reported significant progress regarding the implementation of monitoring tools for preventing cyber threats.
  - Monitoring tools were reported in all cases, but no details of how their performance was provided.
  - 10/12 central banks reported to address gaps in the monitoring tools to improve detection, after assessing results.
  - Half of the respondents confirmed to have a reporting framework for cyber incidents.

- Concerning intelligence (and information) sharing, LAC central banks basically receive information
  - It was not surveyed if received information is being used to report back the financial system.
  - Half of the central banks have available a platform where internal and external stakeholders can share the last updates and information about cyber threats, training, testing and related activities. 1 of 4 central banks have an outsourced platform for this purpose.

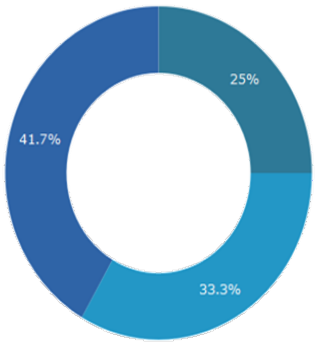
Detection and testing

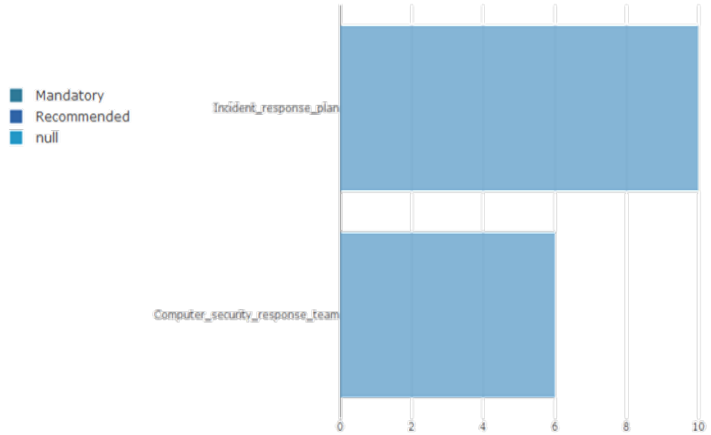
- The range of tools that central banks reported to be used for detection are wide
  - Simulated attacks and a threats detection system (monitoring users) were mentioned by almost all (11/12) to measure vulnerability and resilience
  - Almost half of the central banks do not have metrics, nor historical records.
- Concerning penetration tests an equal number of central banks use external and internal exercise, while simulations in the payment systems are less common. (see chart)



Incident response

- An incident response plan is available in 5 of each 6 central banks. (left chart)
- Only in half of the LAC central banks, an incident response team (external or internal) is available. (left chart)
- Concerning communication aspects during and after an event, a number of countries (1/3) have not a plan.
  - Informing relevant actors is critical to ensure continuity and resilience,
  - Only 25 of the central banks have a mandatory plan including communication. (right chart)





CEMLA
CENTRO DE ESTUDIOS MONETARIOS LATINOAMERICANOS

Recovery

- Plan to recover can be made of several actions, but the LAC central banks rely much more on making regular back-ups (11/12) and ensuring capacity to restore critical data or systems.
  - Central banks reported that ensuring availability of critical information is closely related to recovery capacity. 3 of 4 central banks can do this from zero.

- The existence of an emergency plan to install patches, change passwords and tuning the networks and transmission channels is a weaker aspect against other measures for recovery.
  - Less than half of central banks reported to have robust monitoring (and follow up) for repeated attacks affecting other vulnerable functions.

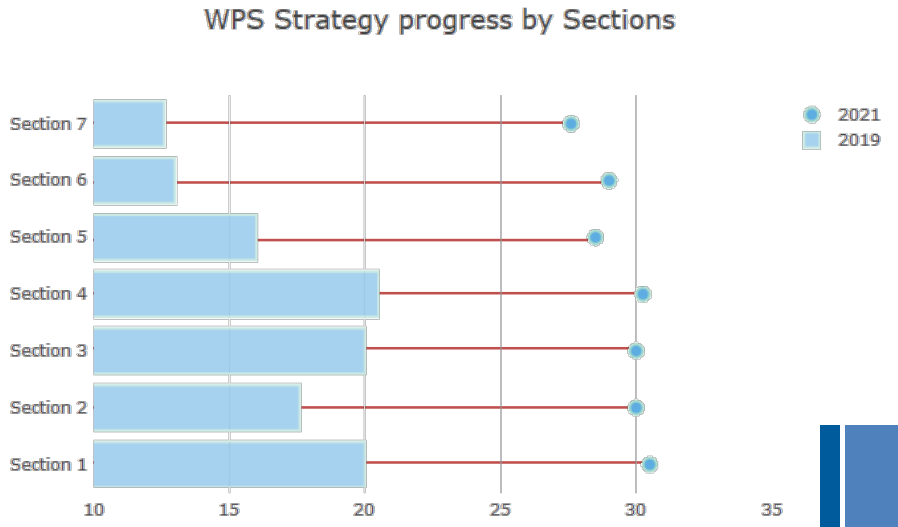
Learning and adapting

- Besides using records and testing, skills are much useful at central banks, but only 3/4 are prepared to respond a cyber attack.
  - Cloud security is a skill at grow with only 3/12 central banks reporting to have staff skilled for using cloud services
  - Risk management skills stemming from Information Security is the most significant human resource available in each 5 of 6 central banks of the region.
- Training programs, despite the above, are available in 10/12 central banks of the región.
  - Only 1 central bank reported to have a training program for stakeholders.
  - It was not surveyed, whether a council (incl. Relevant stakeholders) on cyber issues is available, and if this can be used as a vehicle for training.

The CPMI WPS Strategy in LAC

- The elements of the CPMI WPS Strategy that will be better progressed between 2019 and 2021, are:
  - Identifying and understanding the range of risks;
  - Establishing endpoint requirements; and
  - Promoting adherence.

- "Responding in a timely way to potential fraud" and "Support ongoing education, awareness and information-sharing" are the elements that will be much better in 2021 than now.
  - But the template does not allow to measure which specific actions will be taken to get there; and
  - Reported status by 2021, in some cases, are based on expectations.



Final considerations

- Buy-in at the top is important.
  - Cyber risk should be embedded into the Board's agenda.
- Governance arrangements are decisive.
  - Communication within the central bank is critical to ensure that general guidelines (set by the Committee) and policies and rules (set by the cyber security area) are met.
- Awareness among staff should be part of any efforts to strengthen cybersecurity.
  - Many cyber attacks use entry points that are human driven. Training for all the staff must be pursued.
- Regulations should require entities, third parties and other stakeholders to develop an effective, testable and proactive framework
  - Promote further collaboration with the industry to enhance cybersecurity practices
- Pursue cross-border cooperation and harmonization of practices.