CEMLA
CENTRO DE ESTUDIOS MONETARIOS LATINOAMERICANOS

Cyber Resilience and CPMI WPS Strategy in LAC Central Banks

Regional Payments Week

Raúl Morales and Gerardo Gage
CEMLA

20 November 2019, Willemstad

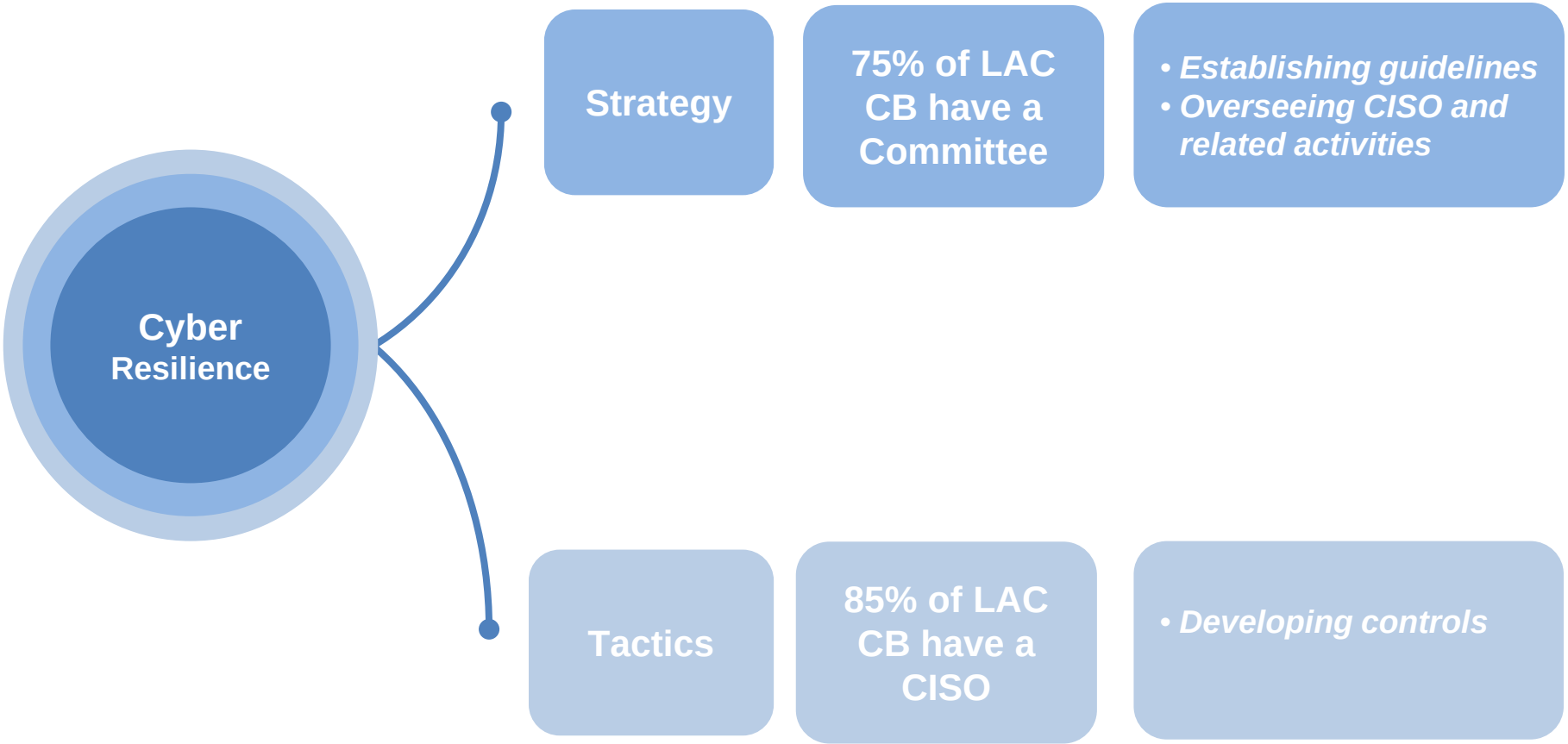
Cyber resilience in LAC Central Banks

2019 Regional survey on cyber resilience practices

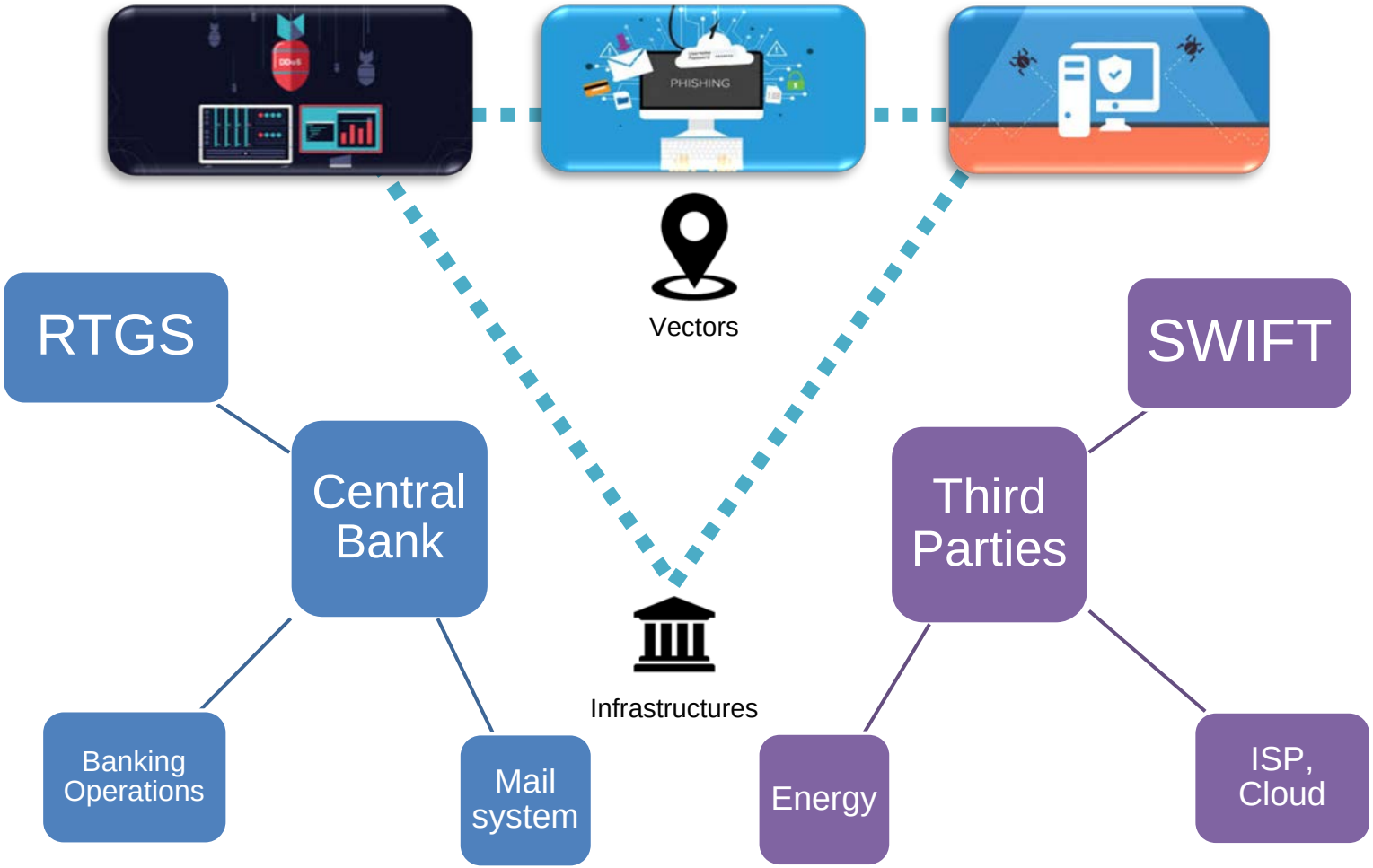
- 12 Central banks
  - 9 Latin American, 3 Caribbean
- 100% of them are:
  - Developing (or already have) its current cybersecurity strategy/framework, following international standards.
  - Implementing monitoring tools for cyber threats detection.
  - Agreed with the CPMI definition on cyber risk.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

CEMLA
CENTRO DE ESTUDIOS MONETARIOS LATINOAMERICANOS

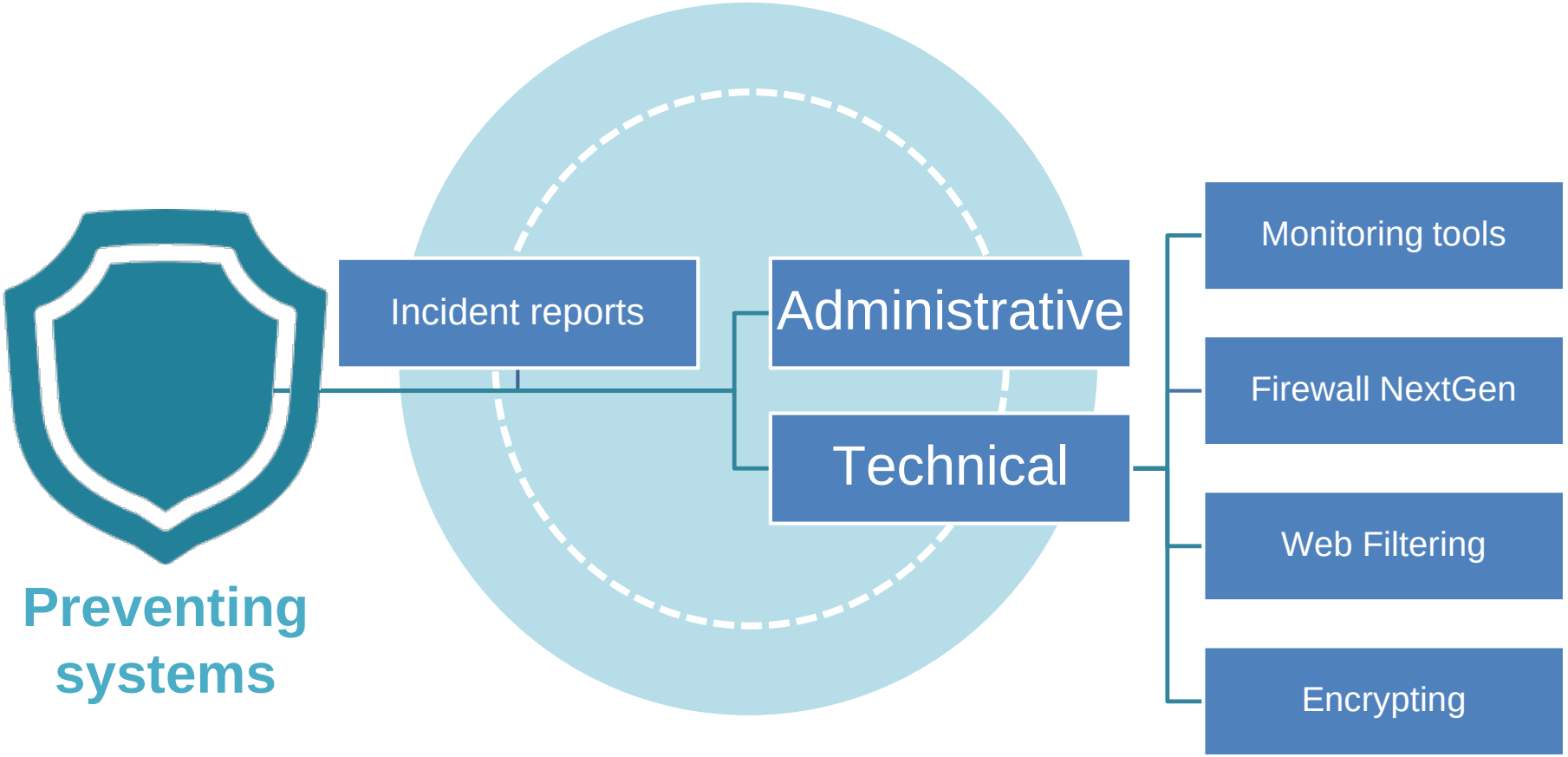
Governance


Cyber Resilience
Strategy
75% of LAC CB have a Committee
• Establishing guidelines
• Overseeing CISO and related activities
Tactics
85% of LAC CB have a CISO
• Developing controls

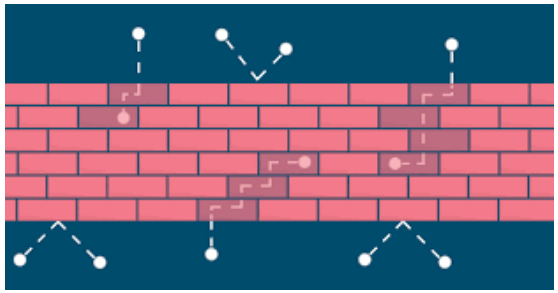
Risks identification



Protection


Incident reports
Administrative
Technical
Monitoring tools
Firewall NextGen
Web Filtering
Encrypting
Preventing systems

Detection and testing



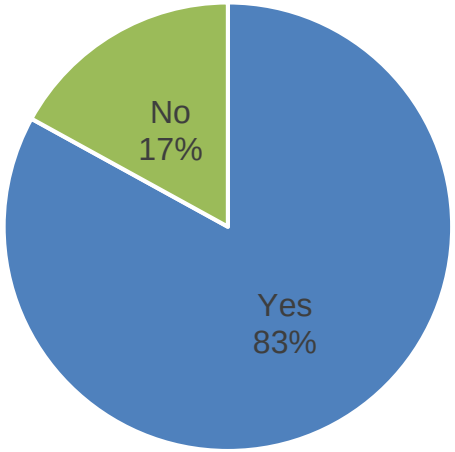
Main vulnerabilities

- Misconfiguration
- Authentication
- Obsolete legacy systems
- Others (SQL injection, EOL, XSS)

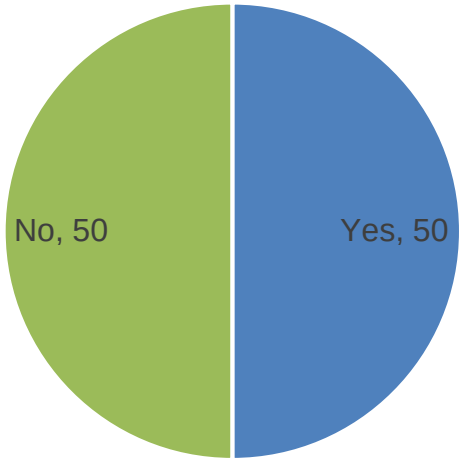
Incident response and recovery

Identifying	Triage	Investigation	Remedy	Post-event
• CSIRT • User Service Manager • CISO • Staff	• CSIRT • Staff • PR & Communications • IT Security & IT • CISO	• CSIRT • Expert team • IT Security & IT • CISO • PR & Communications	• CSIRT • Expert team • IT Security& IT • CISO • PR & Communications	• CSIRT • IT Security & IT • CISO • PR & Communications

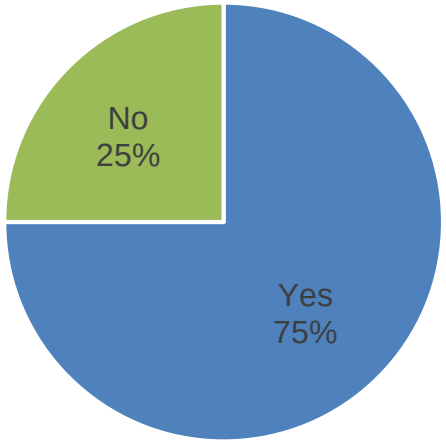
Incident Response Plan



CSIRT



Recovery Capacity



CEMLA
CENTRO DE ESTUDIOS MONETARIOS LATINOAMERICANOS

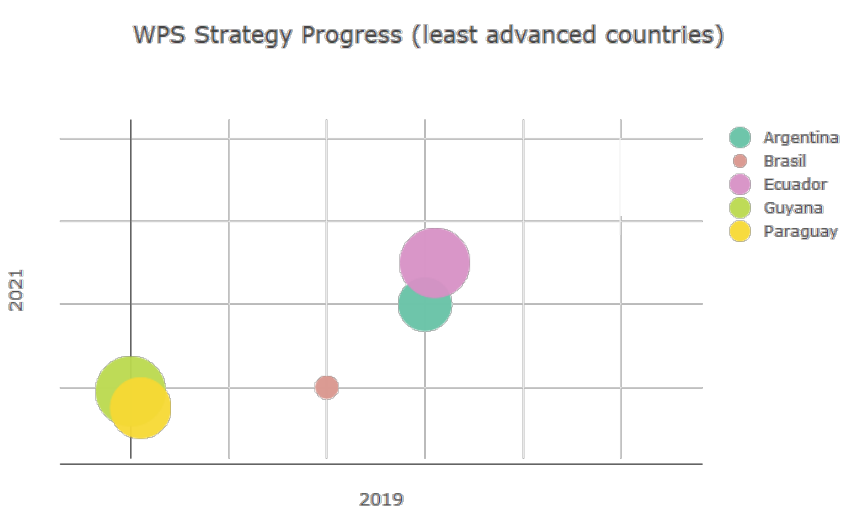
Learning and adapting

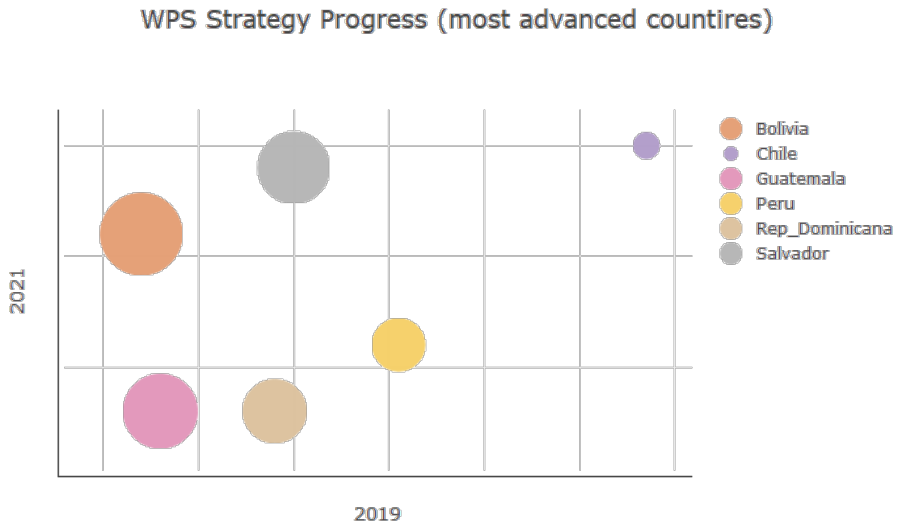
- Besides using records and testing, skills are much useful at central banks, but only 3/4 are prepared to respond a cyber attack.
  - Cloud security is a skill at grow with only 3/12 central banks reporting to have staff skilled for using cloud services
  - Risk management skills stemming from Information 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.

Monitoring efforts to adopt WPS Strategy in LAC

Strategy operationalization (by country)

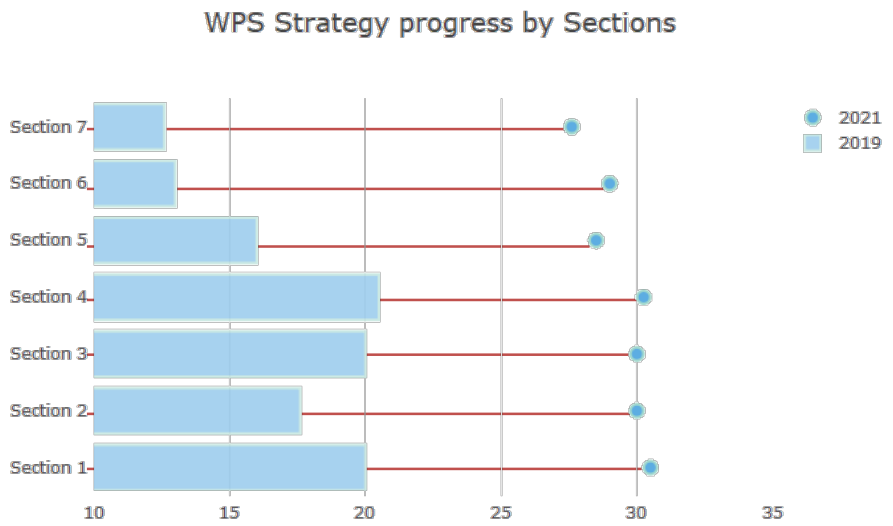
- The jurisdiction that currently reports the greatest progress in implementing the strategy is Chile, followed by Peru.
- Bolivia and El Salvador are the jurisdictions reporting the greatest changes from 2019 to 2021.
- On the other hand, Guyana and Paraguay reported the higher number of cases where the situation is, and will be, on Stage 0.





Strategy operationalization (by element)

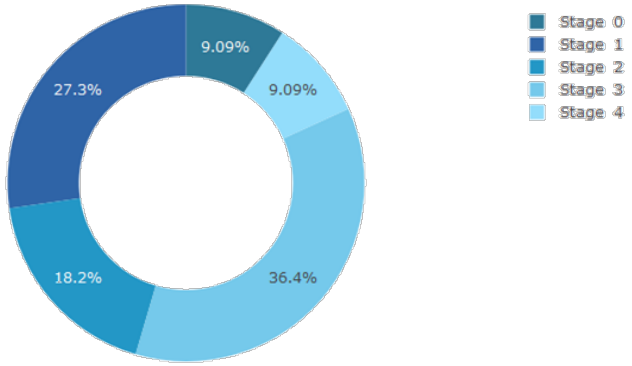
- The elements of the CPMI WPS Strategy that will be better progressed between 2019 and 2021, are:
  - Identify and understand the range of risks (Element 1)
  - Provide and use information and tools to improve prevention and detection (Element 4).
  - Establish endpoint security requirements (Element 2)
- But, where the major changes are seen, Elements 6 and 7 “Support ongoing education, awareness and information-sharing” and “Learn, evolve and coordinate”.



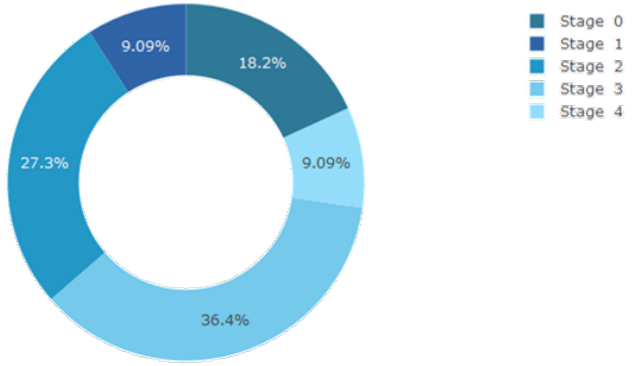
Elements that are better covered

- PSO establishing specific requirements for PSP is the action reported as the most advanced, most of the jurisdictions, however, the majority report Stage 3.
- PSO using tools and info to prevent fraud is the second most advanced action in the region.
- Although these actions show the greatest advance compared with the rest, the proportion of jurisdictions reporting Stage 4 is very low.

PSO establishing specific requirements for PSP



PSO using tools and info to prevent fraud



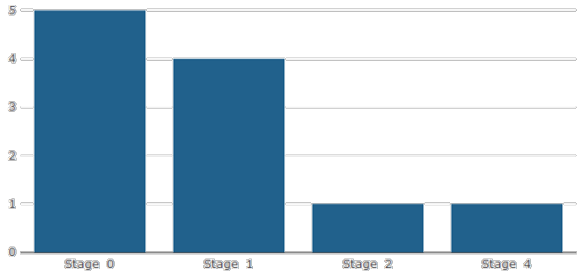
PSO: WPS Operator; PSP: WSP participants.

Where the major gaps are found

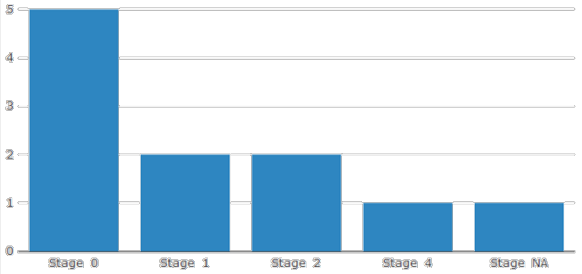
- The actions that were reported as the least advanced (almost 50% of countries reporting Stage 0) are:
  - PSO has established requirements for PSP to alert the community on evolving fraud threats.
  - PSO and PSP seek to coordinate approaches for strengthening endpoint security with other relevant systems and networks.
  - Expectations and assessment programmes reflect the relevant intended outcomes of the strategy.

- PSO requirements for PSP to alert the community on fraud threats, is the action -that considering Stage 1- that is the least advanced among the above three.

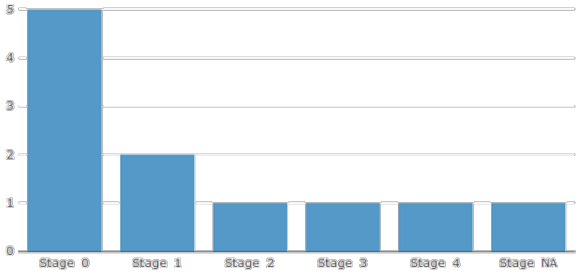
PSO establish requirements for PSP to alert the community on evolving fraud threats



PSO and PSP seek to coordinate approaches for strengthening endpoint security with other relevant systems and networks



Expectations and assessment programs reflect the relevant intended outcomes of the strategy.



CEMLA
CENTRO DE ESTUDIOS MONETARIOS LATINOAMERICANOS

Concerns looking ahead

- The monitoring template does not allow to measure how specific actions will help to reach the expected outcome
  - Reported status by 2021 is a proxy based on expectations.
- LAC central banks reported complexity to interpret the Strategy examples and actions.
  - Some central banks argued that this could led to a certain degree of discretion.
- As expected, implementation sometimes is based on urgency or risk perceived by each authority.
  - Proper staff skills could play against existing efforts.
- Not clear how to outreach PSP and PSO to ensure adherence.
  - Further guidance was mentioned as necessary in some cases.
- Some central banks mentioned that new entrants and possible changes in FMI access arrangements will suggest that additional guidelines in the Strategy could be considered.