Committee on Payments
and Market Infrastructures

BIS

Mission Possible: Strengthening wholesale security

Morten Bech

Regional Payments Week, Curacao, 20 November 2019

Game plan

- The strategy tree
- Core elements
- Intended outcomes
- Emerging practices
  - Examples: elements 4 and 5
- The toolkit

Strategy in action: the strategy tree

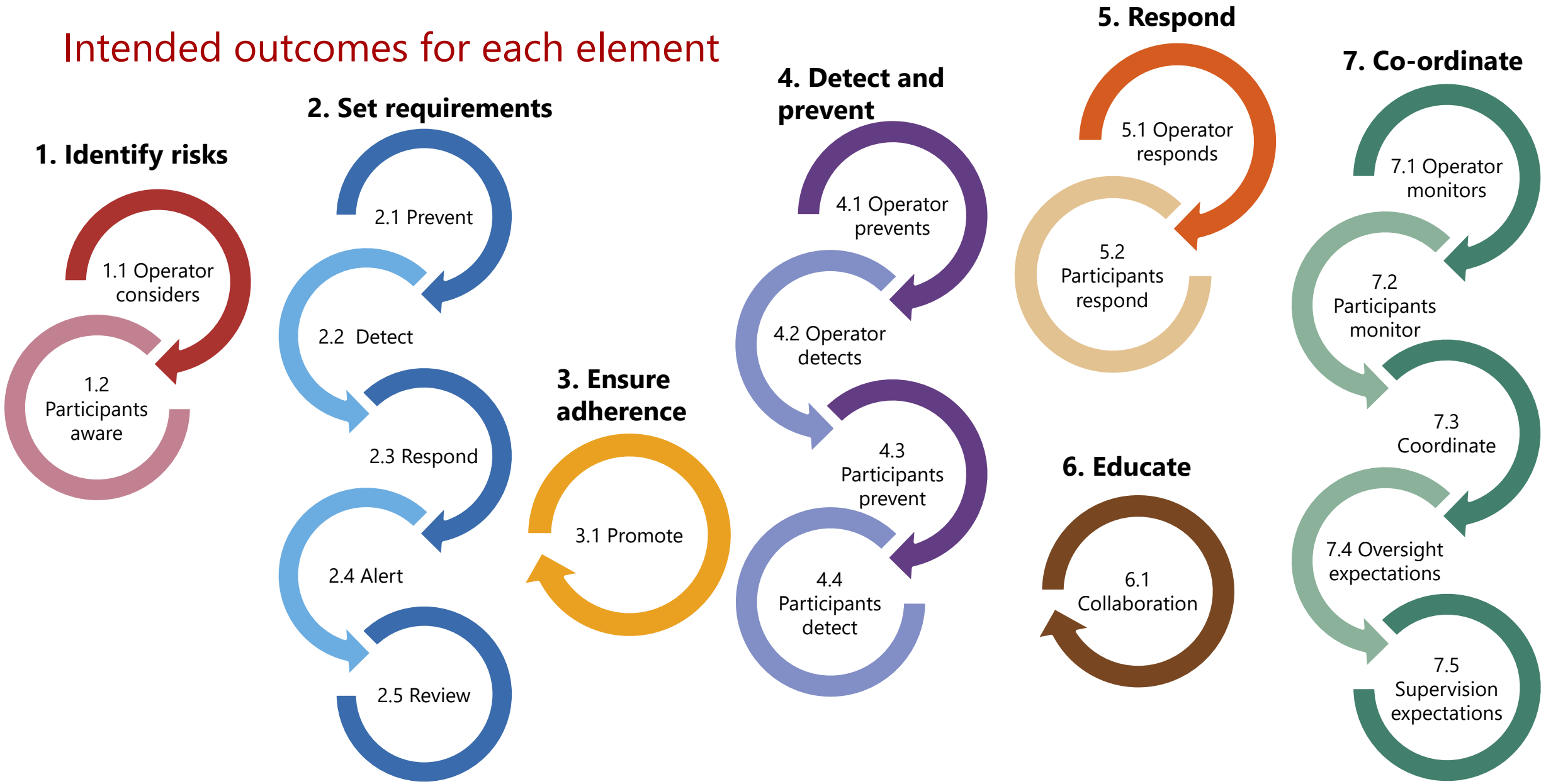
Emerging practices

Intended outcomes

Core elements

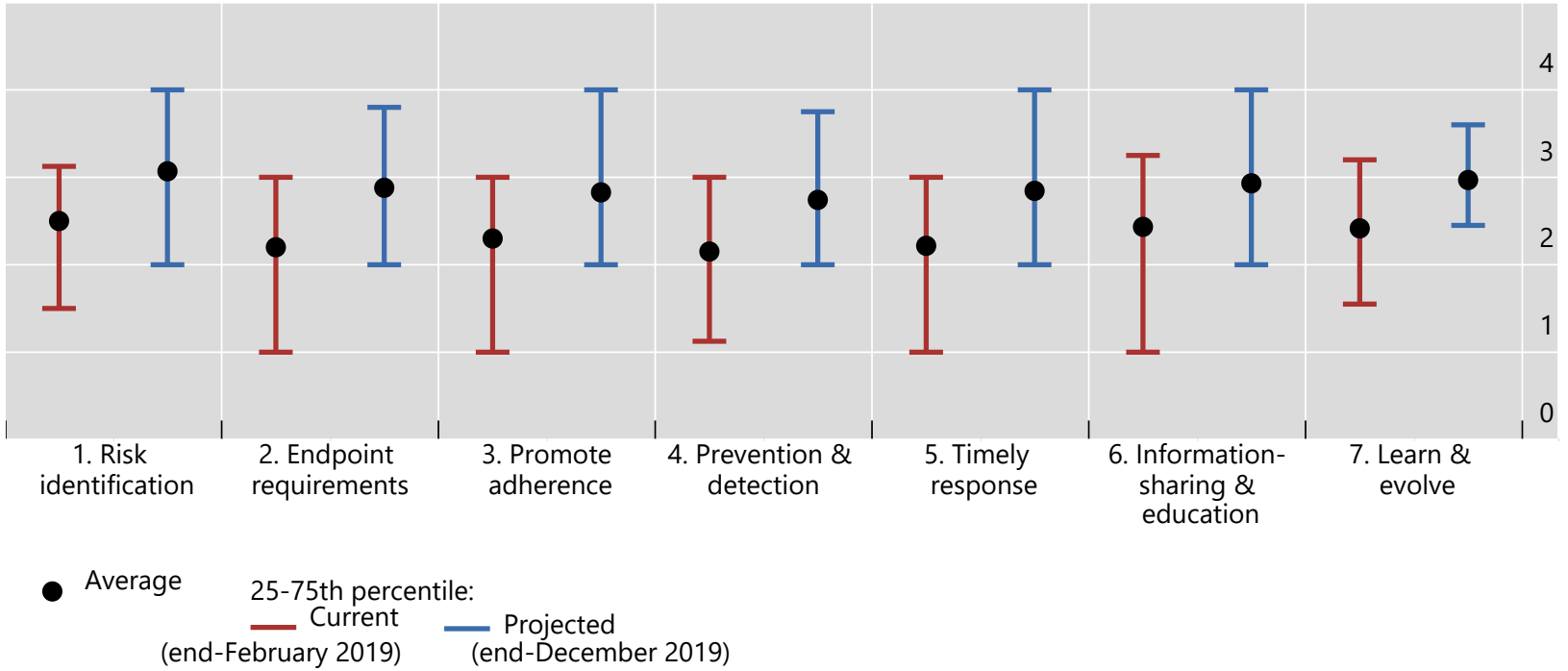
The wholesale payments strategy has 7 core elements

Intended outcomes for each element



To what extent has each elements been operationalised?

Distribution of current and projected states[1]



[1] "0": no assessment of the achievement of the intended outcome. "1": an assessment has begun and actions are being identified to achieve the intended outcome. "2": Assessment completed and actions have been adequately identified to achieve the intended outcome. "3": Intended outcome achieved. "4": Measures put in place to achieve the intended outcome continuously over time.

Source: Reducing the risk of wholesale payments fraud to endpoint security survey 2019.

Emerging practices

Element 4: Prevent and detect – emerging practices

4.1 – 4.2 Operator

Uses information and tools to…

Identify and block fraud payments before processing in real-time.

Identify and investigate fraud payments after processing

Authenticate and prevent settlement of anomalous transactions.

Block fraud transaction that are waiting for settlement on instruction.

Allow whitelists of participants who can be sent funds. Automated intelligence sharing.

4.3 - 4.4 Participant

Uses information and tools to…

Identify and block fraud payments in real time, before they are sent.

Identify and investigate fraud payments after they are sent

Internal tools or external tools (provide by operator or third party).

Ex-post "out of band" reports of sent payments and notices of changes to access credentials provided by operator.

Element 4: Prevent and detect - emerging practices

4.5 Operator

Provides tools to participants and changes settings to…

Identify and block fraud payments in real time. Pre-select the most restrictive settings for participants. Each participant can adjust its settings based on activity/judgement

4.6 Operator and participants

Take a risk based approach with using tools and information to…

Identify and block fraud payments in real time eg from smaller participants and corresponding banking clients

Element 5: Respond- emerging practices

5.1 - 5.2 Operator and Participants

Develop 24/7 emergency hotline, contact lists, internal procedures, tools and staff training to…

Enable the operator to block pending payments that have been identified

Enable each participant to initial and respond to request to block pending payments that have been identified

5.3, 5.5 Operator and Participants

Consider need for and Develop indemnity arrangements to support response to requests to take action, avoiding legal liability.

Employ industry-wide exercises to identify and address potential barriers to a speedy response

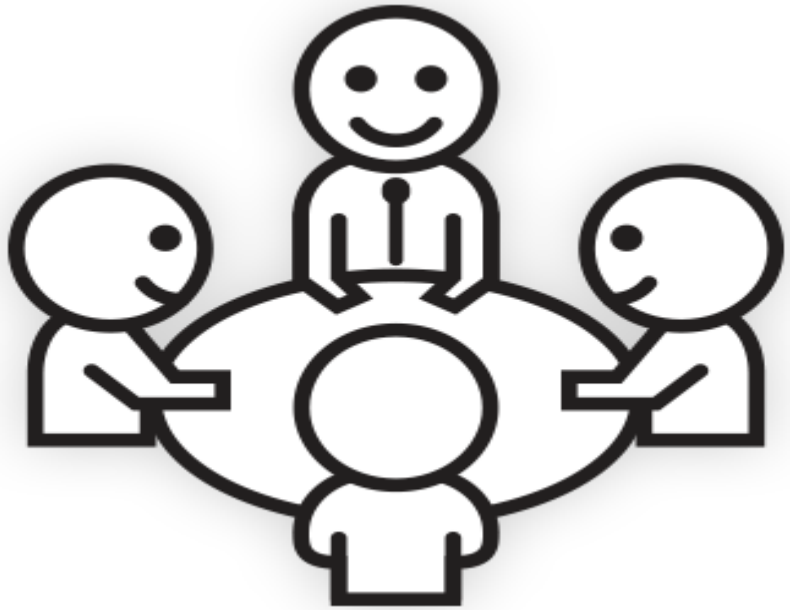
5.4 Participants

Actively engage in industry groups to develop best practices for timely fraud response

We have put together a toolkit to facilitate operationalising of the strategy

FSI online tutorials on the endpoint strategy are also available!

Second industry workshop 3 December 2019, ECB Frankfurt



Progress report. Share emerging practices. Uncover challenges and obstacles. Update the toolkit.