

Effective Practices for Cyber Incident Response and Recovery

ASBA-CEMLA-FSI Virtual Event on Cyber Security

Yasushi Shiina

4 November 2020



Note: The views expressed in this document are those of the author and do not necessarily reflect those of the FSB.

FSB work on enhancing cyber resilience

Enhancing cyber resilience has been a key element of the FSB's work programme to promote financial stability.

- Oct. 2017 *Stocktake on cybersecurity regulatory and supervisory practices*
- Nov. 2018 *Cyber Lexicon*
- April 2019 *Cyber Incident Response and Recovery: Progress Report to the G20 Finance Ministers and Central Bank Governors*
- April 2020 *Effective Practices for Cyber Incident Response and Recovery: Consultative Document*
- Oct. 2020 *Effective Practices for Cyber Incident Response and Recovery: Final Report*

Cyber incident response and recovery (CIRR)

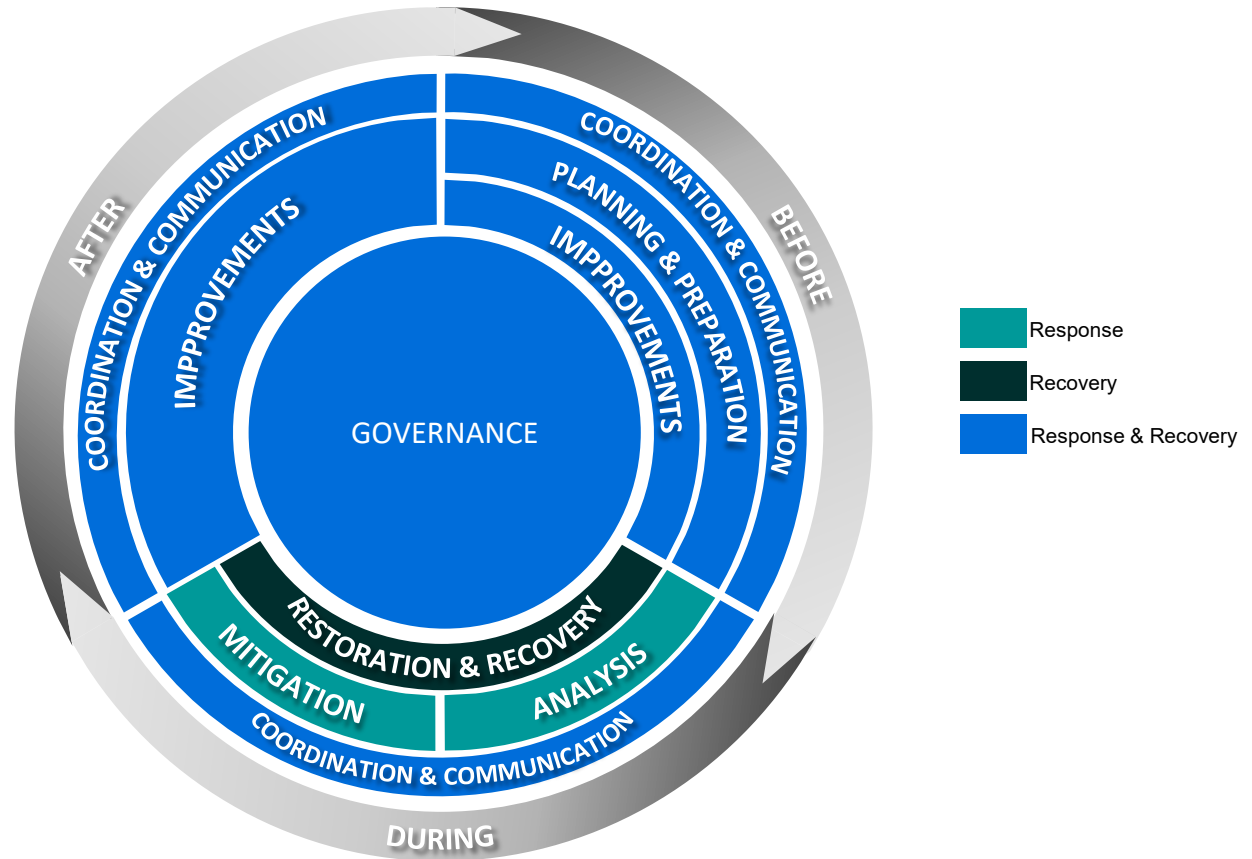
Objective: To develop a toolkit to provide financial institutions with a set of effective practices to *respond to and recover from a cyber incident* to limit any related financial stability risks.

The toolkit is:

- focused on *respond* and *recover* functions.
- designed as *a range of effective practices* that any organisation can choose from, based on its size, complexity and risks.
- not intended to create an international standard, or constitute standards for organisations and their supervisors.
- not a prescriptive recommendation for any particular approach.
- based on (i) survey responses from national authorities, international organisations and external stakeholders; (ii) literature review; and (iii) engagements with stakeholders (including public consultation and lessons from the COVID-19 crisis).

CIRR toolkit: An overview

49 Effective practices across seven components:



Source: FSB (2020) *Effective Practices for Cyber Incident Response and Recovery: Final Report*, 19 October

CIRR toolkit: Components (1)

- 1) Governance: frames the way in which CIRR is organised and managed.
- 2) Planning and preparation occur before an incident and play a significant role in determining the effectiveness of CIRR activities, through establishing and maintaining capabilities to respond to cyber incidents, and to recover and restore critical activities, systems and data affected by cyber incidents to normal operations.
- 3) Analysis includes forensic analysis, and determine the severity, impact and root cause of cyber incidents to drive appropriate and effective CIRR activities.
- 4) Mitigation measures are activated to prevent the aggravation of the situation and to eradicate cyber incidents in a timely manner to alleviate their impact on business operations and services.

CIRR toolkit: Components (2)

- 5) Restoration and recovery restore systems or assets affected by a cyber incident to safely recover business-as-usual operations and delivery of impacted services.
- 6) Coordination and communication with trusted or relevant stakeholders (including authorities) allow organisations to maintain good cyber situational awareness and enhance the cyber resilience of the ecosystem in which they operate across the life cycle of a cyber incident. Close coordination with relevant stakeholders throughout the CIRR life cycle enables timely communication of progress and outcomes of the CIRR activities.
- 7) Improvement establishes processes to improve CIRR activities and capabilities through lessons learnt from both proactive tools (e.g. CIRR exercises, tests and drills) and past cyber incidents.

CIRR toolkit: Example of tools (1)

1) Governance (tools #1-9):

- Establish organisation-wide governance framework
- Define specific/clear roles and responsibilities of the board and senior management as well as for overall CIRR activities
- Identification of CIRR coordinator
- Promote executive sponsorship
- Cultivate the right culture
- Ensure CIRR investment
- Establish metrics to measure impact of the incident to determine the severity and priority of the incident.
- Provide adequate resources (for both staffing and competencies)

CIRR toolkit: Example of tools (2)

2) Planning and preparation (tools #10-20):

- Establish policies that involve organisation's functions in CIRR.
- Establish and maintain well-planned plans and playbooks.
- Establish communication strategies, channels and plans for internal and external stakeholders.
- Inclusion of severe but plausible cyber scenarios and stress tests in plans and playbooks.
- Manage evaluation and record of incidents.
- Security Operations Centre (SOC), IT disaster recovery and infrastructure resilience,
- An effective log management and forensic capabilities
- Management of third-party service providers and supply chain.

CIRR toolkit: Example of tools (3)

3) Analysis (tools #21-23):

- Use pre-defined cyber incident taxonomy.
- Retrieve system and transaction logs.
- Correlate trusted internal and external information sources.

4) Mitigation (tools #24-27):

- Apply containment measures best suited to each type of incidents (e.g. use of Indicators of Compromise (IoC)).
 - Business continuity measures
 - Isolation
 - Eradication

CIRR toolkit: Example of tools (4)

5) Restoration and recovery (tools #28-35):

- Prioritisation of recovery activities based on criticality of business etc.
- Ensure data restoration (e.g. “golden source” data).
- Establish approved restoration procedures.
- Define key milestones to redesign, reinstall and reconfigure systems in CIRR plans.
- Tracking and monitoring of restoration process and recovery progress.
- Validation of the restored assets.
- Document and timestamp actions taken from the time the incident was detected to its final resolution.

CIRR toolkit: Example of tools (5)




6) Coordination and communication (tools #36-42):

- Timely escalation of cyber incidents to internal stakeholders based on agreed severity assessment framework
- Relevant cyber incident reporting in line with national requirements
- Regular updates to stakeholders with messages that are actionable, accurate, timely, clear and relevant.
- Engagement with the media using a pre-defined communications strategy and cross-functional communication team.
- Adoption of FSB Cyber Lexicon and other commonly used taxonomies.
- Sharing of information on significant cyber threat intelligence, cyber incidents, effective cyber security strategies and risk management practices.
- Use of trusted, secure communication channels.

CIRR toolkit: Example of tools (6)

7) Improvements (tools #43-49):

- Collaboration with industry-wide initiatives.
- Post-incident analysis of the effectiveness of established procedures and actions taken.
- Conduct exercises, tests and drills on a regular basis (tabletop exercises, live simulations).
- Participation in cross-border and cross-sectoral exercises.
- Use of technological aids (e.g. automation tools)

 +41 61 280 8844
 fsb@fsb.org
 www.fsb.org/contact

 @FinStbBoard
 FinancialStabilityBoard

The Financial Stability Board (FSB) is established to coordinate at the international level the work of national financial authorities and international standard-setting bodies in order to develop and promote the implementation of effective regulatory, supervisory and other financial sector policies. Its mandate is set out in the FSB Charter, which governs the policymaking and related activities of the FSB. These activities, including any decisions reached in their context, shall not be binding or give rise to any legal rights or obligations under the FSB's Articles of Association.

FSB