FSB FINANCIAL STABILITY BOARD

Effective Practices for Cyber Incident Response and Recovery

Final Report

19 October 2020

The Financial Stability Board (FSB) coordinates 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.

Contact the Financial Stability Board

Sign up for e-mail alerts: www.fsb.org/emailalert
Follow the FSB on Twitter: @FinStbBoard
E-mail the FSB at: fsb@fsb.org

Table of Contents

Executive summary

Cyber incidents[1] pose a threat to the stability of the global financial system. In recent years, there have been a number of cyber incidents that have significantly impacted financial institutions and the ecosystems in which they operate.[2] A significant cyber incident, if not properly contained, could seriously disrupt the financial system, including critical financial infrastructure, leading to broader financial stability implications.

Efficient and effective response to and recovery from a cyber incident by organisations in the financial ecosystem are essential to limit any related financial stability risks. Such risks could arise, for example, from interconnected IT systems between multiple financial institutions or between financial institutions and third-party service providers, from loss of confidence in a major financial institution or group of financial institutions, or from impacts on capital arising from losses due to the incident. The cyber resilience of organisations is crucial for the smooth functioning of the financial system and in engendering financial stability.

Enhancing cyber incident response and recovery (CIRR) at organisations is an important focus for national authorities. National authorities are in a unique position to gain insights on effective CIRR activities in financial institutions from their supervisory work, and their observations across multiple organisations can help suggest areas for enhancement. Authorities also have an important role to play in responding to cyber incidents that present potential risks to financial stability. Authorities can consider the sector-wide implications of a cyber incident or series of cyber incidents, including any market confidence issues and reactions resulting from information from public market data, news and social media, or from partial or inaccurate information, possibly proliferated by fraudulent sources. Authorities may also, as appropriate, support organisations in sharing information to protect against threats that could have a detrimental impact on financial stability.

The FSB has developed a toolkit of effective practices that aims to assist organisations in their cyber incident response and recovery activities. In this regard, organisations' respond function executes the appropriate activities in reaction to a detected or reported cyber incident, while the recover function carries out the appropriate activities to restore any systems, capabilities or resume services or operations that were impaired due to a cyber incident.[3]

The FSB encourages authorities and organisations to use the toolkit to enhance their CIRR activities.

---

1 A cyber incident is a cyber event that:
(i) jeopardizes the cyber security of an information system or the information the system processes, stores or transmits; or
(ii) violates the security policies, security procedures or acceptable use policies,
whether resulting from malicious activity or not. See FSB (2018) *Cyber Lexicon*, November, page 9.

2 The twin episodes of the NotPetya and the WannaCry ransomware attack in 2017, for example, showed the potential of cyber incidents to be both widespread and devastating.

3 FSB (2018), page 12 for definitions of the Respond and Recover functions.

Introduction

Enhancing cyber resilience has been a key element of the FSB's work programme to promote financial stability. In 2017, the FSB took stock of financial sector cyber security regulations, guidance and supervisory practices.[4] This work identified, among other things, a need to enhance communication between authorities and the private sector. To facilitate more effective communication, the FSB developed a Cyber Lexicon in 2018 to support the work of the FSB, standard-setting bodies (SSBs), authorities and private sector participants to address financial sector cyber resilience.[5]

Given the interconnectedness of the financial sector, the FSB agreed in 2018 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 not intended to create an international standard, or constitute standards for organisations and their supervisors. It is not a prescriptive recommendation for any particular approach. The toolkit is designed as a range of effective practices that any organisation can choose from, based on its size, complexity and risks.

Development of the toolkit

The draft toolkit of effective practices was published on 20 April 2020 for public consultation.[6] In developing the consultative document, the FSB conducted a stocktake of publicly released guidance from national authorities, international organisations and other external stakeholders;[7] reviewed existing standards and case studies on past cyber incidents and engaged with external stakeholders at workshops and bilateral meetings. The FSB also drew on insights from national authorities based on their supervisory work.

The public consultation period ended on 20 July 2020, and 58 responses were received from a wide range of external stakeholders, including banks, insurers, financial market intermediaries, industry associations, IT service providers and public authorities.[8] Through the public consultation and engagements with external stakeholders, the FSB sought feedback on lessons learnt from the COVID-19 pandemic and related cyber activity. Thus far, organisations and authorities have generally responded well and shown resilience to cyber risk. This in part reflects the degree to which organisations practiced their playbooks, conducted stress tests and cyber drills, and actively maintained contact lists of key external and internal stakeholders. However, the COVID-19 pandemic also highlighted the need for many organisations and authorities to consider adjustments to cyber risk management processes, cyber incident reporting, cyber incident response and recovery activities, as well as management of critical third-party service providers (e.g. cloud services) and relevant stakeholders. Effective preparation and testing of incident response and recovery plans, particularly business continuity planning, facilitated organisations' transition to remote work and operations. One of the key challenges posed by

---

4 FSB (2017), *Summary Report on Financial Sector Cyber security Regulations, Guidance and Supervisory Practices*, October.

5 FSB (2018).

6 FSB (2020), *Effective Practices for Cyber Incident Response and Recovery: Consultative document*, 20 April.

7 For example, a survey of industry practices was conducted in July 2020.

8 All public responses received are available on the FSB website.

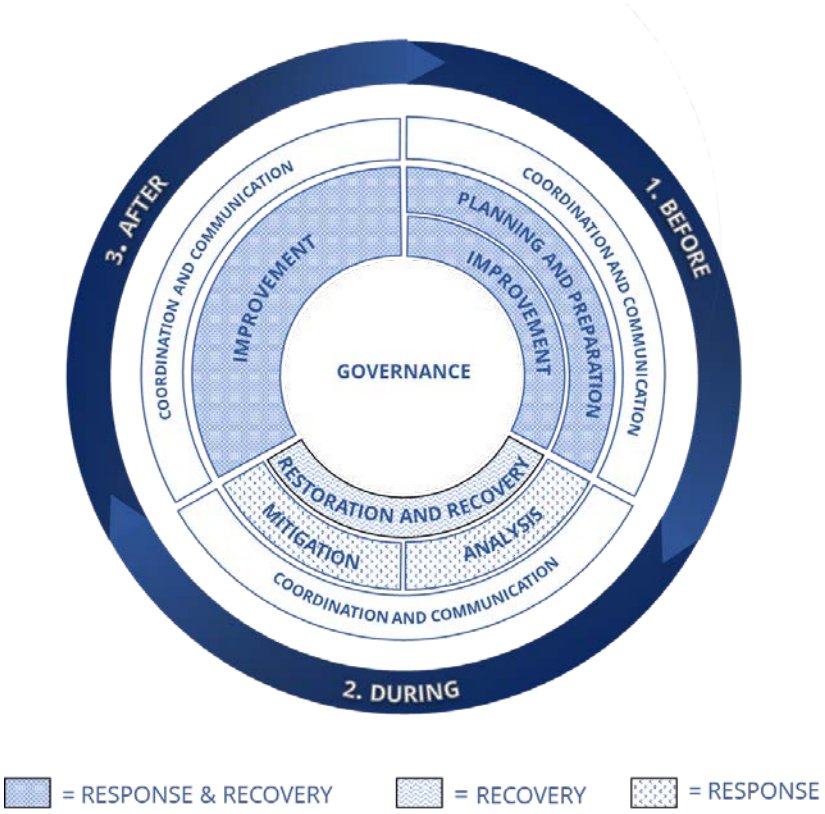
remote working was the restricted ability to collect system hardware in order to conduct forensic analysis of a cyber incident. Furthermore, effective communication across the supply chain, including through intra-group entities and third-party service providers, is often highlighted as a key challenge.

Drawing on the feedback from the public consultation, the FSB modified the draft effective practices in the following ways. First, the FSB further clarified the proportionate and risk-based nature of the toolkit to improve its usability. Second, the toolkit is better aligned with industry practices and international standards. For example, "preparation" and "restoration" components have been renamed "planning and preparation" and "restoration and recovery" respectively, and the details of the relevant effective practices have been modified to more closely align with existing or leading practices adopted by organisations.

The toolkit

The toolkit, structured across seven components, comprises 49 effective practices that organisations have adopted while taking into account jurisdictions' legislative, judicial and regulatory frameworks, the size of the organisation, the organisation's role in the financial ecosystem and the extent to which stakeholders are affected by a cyber incident. The toolkit is composed as a resource and reference guide for effective practices using common cyber-taxonomies in a manner aligned to industry standards accessible to senior management, board of directors or other governance or compliance, risk, and legal professionals that interface with cybersecurity technical experts within the organisation, the SSBs or authorities.

Figure 1: Illustration of CIRR components



While many of these effective practices are already in use by larger organisations, they could also be valuable for smaller and less complex organisations to help strengthen their cyber resilience.[9] The toolkit provides a range of effective practices and organisations can choose to adopt some or all of the effective practices that are suitable for their respective business models, taking into account their size, complexity and risks to the financial ecosystem.[10]

The toolkit is useful for authorities as they consider the approaches they may undertake with respect to regulation or supervision, or in responding to a cyber incident within the sector. The toolkit promotes a common range of effective practices that SSBs and authorities can incorporate into their guidance around cybersecurity.

1. Governance

Governance frames the way in which CIRR is organised and managed. It aligns CIRR activities with goals set for continuity of business operations, sets the organisational structure and roles needed to coordinate response and recovery across internal functions, business lines, organisations, jurisdictions or even sectors. Governance involves defining the decision-making framework with clear steps and measures of success, and allocates responsibilities and accountabilities to ensure that the right internal and external stakeholders are engaged when a cyber incident occurs. Governance also encapsulates the commitment to support CIRR activities through adequate sponsorship by senior management and to promote positive behaviours dealing with, and following, a cyber incident.

1. **Organisation-wide governance framework.** The CIRR governance structure is part of the broader organisation-wide governance framework. CIRR objectives and priorities are aligned with the organisation's risk management framework and are communicated and understood throughout the organisation. Based on the risk management framework, roles and responsibilities are clearly defined for managing CIRR activities and internal processes to facilitate effective decision-making when handling a cyber incident.

2. **Roles and responsibilities of the board and senior management.**[11] Organisations have clear and direct reporting lines between their management and the board (or board of directors) in order to ensure accountability, and the roles and responsibilities of management are clearly specified for CIRR activities.

    - **The board**. The board is responsible for steering the organisation's risk management strategy and sets clear and achievable CIRR objectives to enhance the cyber resilience of the organisation. The board plays a key role in assessing the effectiveness of these

9 FSB (2018), page 9.

10 As the toolkit is a not a one-size-fits-all approach, the onus will be on organisations and authorities to assess whether their governance framework and processes are adequate and their CIRR activities are effective.

11 The toolkit refers to a management structure composed of a board of directors and senior management. There are significant differences in legislative and regulatory frameworks across jurisdictions regarding the functions of the board of directors and senior management. In some jurisdictions, the board has the main, if not exclusive, function of supervising the executive body (senior management, general management) and is known as a supervisory board. This means that the board has no executive functions. In other jurisdictions, the board has a broader competence in that it lays down the general framework for the management of the organisation. Owing to these differences, the terms "board of directors" and "senior management" are used in the toolkit to label distinct decision-making functions within an organisation.

activities in meeting the CIRR objectives and empowers senior management to take decisions to deploy CIRR activities.

- **Senior management**. Senior management is responsible for the implementation of the policies, procedures and controls that support the CIRR activities. Senior management engages with business and technical functions within the organisation to develop, exercise, maintain, manage, support and improve CIRR objectives and plans consistent with organisational needs.

3. **Clear, defined roles for CIRR.** Organisations clearly define the roles, responsibilities and accountabilities for all organisational areas that may be involved in the various CIRR activities. Potential conflicts of interest are minimised by ensuring a separation of implementation and oversight roles where possible.[12] For example, organisations commonly rely on the three lines of defence model that facilitates the segregation of duties, and provides for an independent check and balance, which the board can rely on for an objective assessment of the effectiveness of CIRR activities.[13] Apart from staff who are responsible for the various CIRR activities, organisations identify key roles (among others) to assist in managing the cyber incident. Material operational outages may involve several organisational areas including but not limited to Impacted Business Units, General Counsel, Communications/Public Relations, Risk, and Information and Communication Technology (ICT).

4. **Incident coordinator.** While different teams and individuals are responsible for different aspects of CIRR activities within an organisation, it is useful to identify an individual or a team to coordinate actions and communications for a cyber incident. Depending on the severity of an incident, the incident coordinator or team may trigger CIRR activities and engage decision-makers across the life cycle of a cyber incident. The delegated incident coordinator or team minimises the potential for CIRR respondents to receive conflicting orders or information from different stakeholders, thereby improving the flow of information and aiding the coordination of response and recovery efforts.

5. **Executive sponsorship.** Staff proactively engages senior management on CIRR activities to promote awareness, seek executive-level guidance and share accountability for success. Executive sponsorship can be in the form of financial and non-financial support and is essential to the implementation and execution of effective CIRR activities. For example, regular updates from senior management on the organisation's CIRR efforts is an effective way to keep staff informed and up-to-date on key developments and engender support.

---

[12] For instance, organisations could use a RACI matrix, which is a tabular format for documenting the allocation of Responsible, Accountable, Consulted and Informed roles.

[13] The three lines of defence commonly consists of business unit management, an independent corporate operational risk management function and independent assurance. Depending on the organisation's nature, size and complexity, and the risk profile of an organisation's activities, the degree of formality of how these three lines of defence are implemented will vary. See BCBS (2020) *Consultative Document: Revisions to the principles for the sound management of operational risk*, August.

6. **Culture.** Senior management demonstrates commitment by creating an organisational environment where staff are encouraged to report or escalate cyber incidents to management. Organisations promote such an environment through structured training programmes at all levels including the board and senior management that encourage learning from mistakes, management leading by example and rewarding staff who demonstrate desired behaviours. A positive culture towards cyber incident handling can enable an organisation to shift its focus from trying to suppress incidents towards using these incidents to improve the organisation and enhance its readiness. In light of the flexibility that the business expects, organisations can benefit from a continuous proactive approach towards their CIRR activities, which includes continuous relationships with their service providers and other relevant parties in the supply chain that are necessary for an effective response to and recovery from the incident. Organisations that possess higher levels of maturity and readiness are able to respond with more speed to different cyber incidents and are able to adjust themselves to the evolving situation.

7. **Funding**. The board and senior management view CIRR not simply as a cost to be borne, but as an investment to ensure the security and reliability of financial services; achieving excellence in containment and restoration from cyber incidents is a necessary competitive element for an organisation. Board and senior management allocate sufficient budget to CIRR, including for technology tools and other support, training and communication programmes at all levels of the organisation. CIRR spending is assessed based on the commensurate risks associated with protecting and assuring continuity of critical functions, and potential implications for financial stability. Peer comparison (or benchmarking) can help identify areas where funding should be channelled.

8. **Metrics.** Organisations establish metrics to measure the impact of a cyber incident and to report to management the performance of CIRR activities. Matrices can be used to determine the severity or priority of an incident. The severity level will inform how quickly the incident needs to be handled and to whom it might be escalated. For example, a high or critical severity incident likely needs to be escalated to the board level. A low priority incident could likely be handled by the incident response team alone.

Box 1: Examples of metrics used by industry

- Metrics to measure impact of a cyber incident
  - Duration of unavailability of critical functions and services
  - Number of stolen records or affected accounts
  - Volume of customers impacted
  - Amount of lost revenue due to business downtime, including both existing and future business opportunities
  - Percentage of service level agreements breached
- Performance metrics for incident management
  - Volume of incidents detected and responded via automation
  - Dwell time (i.e. the duration a threat actor has undetected access until completely removed)
  - Recovery Point Objectives (RPOs) and Recovery Time Objectives (RTOs)

9. **Resources.** Organisations ensure that CIRR functions are adequately staffed and the competencies of relevant personnel are maintained and regularly enhanced through structured training programmes, internal job rotations (e.g. between Red and Blue teams) or exchanging staff between organisations, jurisdictions and sectors to broaden their experience and knowledge.

2. Planning and preparation

Organisations establish and maintain capabilities to respond to cyber incidents, and to recover and restore critical activities, systems and data affected by cyber incidents to normal operations. Planning and preparation occur before an incident and play a significant role in determining the effectiveness of CIRR activities.

10. **Policies.** Organisations establish policies that define the involvement of the organisation's functions in the CIRR process. The policies are based on regulatory, legal and business requirements and are enforced at all levels of the organisation, according to its size, complexity and risks, with coherence across relevant jurisdictions where the organisation operates. Policies include relevant high-level statements that drive the development of more detailed plans and playbooks. For instance, policies should, among other things, address the classification and the assessment of cyber incidents and include a clear communication strategy and plan, which describe whom to inform of the cyber incident within a given timeframe.

11. **Plans and playbooks.** Organisations establish and maintain plans and playbooks that provide well-defined, organised approaches for CIRR activities, including criteria for activating the measures to expedite the organisation's response time. Plans and playbooks are developed in consultation with business lines to incorporate business recovery requirements and to clearly identify the impact on customers. Senior management approves plans and playbooks before they are broadly shared across the organisation. They are reviewed and updated regularly to reflect improvements, or changes in the organisation and results of any relevant risk assessment. Organisations enlist internal or external subject matter experts to review complex and technical content, where appropriate. Organisations develop a number of plans and playbooks for specific purposes (e.g. response, recovery, contingency, communication) that align with the overall cyber resilience strategy that uses a common taxonomy. Plans and playbooks cover the initial hours and days of a cyber incident, which are usually the most critical.

12. **Communication strategies, channels and plans.** Organisations establish lists of internal and external stakeholders to be informed depending on identified scenarios and criteria, such as on the severity of the incident as well as any required regulatory and statutory notifications. Organisations establish their communication strategies for internal and external stakeholders. They develop a communications plan and drawer statements to address different types of cyber incidents, with consideration of the appropriate and available communication channels (e.g. mainstream media, social media). Organisations also prioritise and sequence information sharing with internal and external stakeholders during an incident. This includes differentiating those stakeholders involved in CIRR activities and those that need to be kept informed. Effective prioritisation reduces uncertainty

and increases credibility with stakeholders, mutual understanding and a constructive approach (i.e. reducing blaming and negative criticism).

Box 2: Examples of internal and external stakeholders

- **Internal stakeholders** are involved in multidisciplinary CIRR activities according to the type of cyber incident and the criticality of their function as well as those that need to be informed of the incident. These include:
  - board members, senior management
  - business lines
  - technical support teams
  - public relations officers
  - legal and compliance officers
  - customer service desks
- **External stakeholders** that may be impacted or that need to be involved in CIRR activities depending on the type of cyber incident. These include:
  - financial counterparties
  - financial market infrastructures (FMIs)
  - customers
  - third-party service providers
  - relevant authorities
  - general public
  - National Cyber Emergence Response Team (CERT) or Cyber Security Incident Response Team (CSIRT)

13. **Scenario planning and stress testing.** Organisations' plans and playbooks include severe but plausible cyber scenarios and stress tests that are based on high-impact, low-probability events and scenarios led by cyber threat intelligence that may result in service failure. Common cyber scenarios include ransomware, Distributed Denial of Service (DDoS),[14] system intrusion, data exfiltration and system disruption. Organisations regularly use threat intelligence to update the scenarios so that they remain current and relevant. These scenarios and stress tests are regularly assessed in business continuity tests and CIRR exercises. Organisations plan and perform such exercises according to their size, complexity and risks. Where appropriate, stress tests involve key external stakeholders, such as relevant authorities and third-party service providers.

14. **Incident evaluation and records management.** Organisations evaluate the effectiveness of CIRR activities during tests and actual incidents. They appoint an independent observer(s) to maintain an accurate record of the cyber incident throughout its different

[14] FSB (2018), page 10.

phases, as well as documenting actions and decisions taken during and after a cyber incident. In some cases, they can utilise voice or video recording. The record serves as an accurate source of reference for the organisation and promotes understanding and effectiveness of the response and recovery actions taken. In addition, the record facilitates after-action reviews to improve future CIRR activities.

15. **Security Operations Centre (SOC).** Depending on their size, complexity and risks, organisations operate a 24x7 SOC or engage third-party security services to meet the needs of the organisation to detect, identify, investigate and respond to cyber incidents that could impact the organisation's infrastructure, services and customers. Various tools, including machine learning, are used for vulnerability management and compliance monitoring to enhance the effectiveness of cyber incident analysis.

16. **IT disaster recovery and infrastructure resilience.** Organisations build resilience through use of diversified infrastructure (e.g. for power and telecommunications infrastructure that could be affected by cyber attacks) and replicate critical systems and data to disaster recovery sites and alternative sites with different geographical risk profiles. Organisations identify concentration risk for external arrangements, and evaluate and adopt mitigation techniques, where available. Organisations choose to backup and store critical data in offline systems that effectively shield the data asset from unauthorised access and data corruption by intentional or unintentional alterations. Organisations invest in technology to enhance their recovery capability. Failover tests and recovery tests are performed regularly to validate effectiveness of these measures for ensuring availability and integrity of data and systems.

17. **Log management and forensic capabilities.** Organisations develop an effective log management and retention framework that is comprised of tools to manage, collect and store system logs that would be required to facilitate incident investigation and analysis. The types of logs to be collected and retention period of logs could be pre-determined based on supervisory rulemaking, law, or the importance of the business data held or transported through the system. Organisations establish technical and forensic capabilities to preserve evidence and analyse control failures, identify security issues and other causes related to a cyber incident. If the organisation does not have its own forensic capabilities, contractual agreements with third-party service providers are established (e.g. forensic retainer services) to support extended cyber forensic investigations, which are immediately activated when needed. Staff who perform forensic work are adequately trained and adhere to robust forensic procedures to safeguard the integrity of the evidence, data and systems during investigations.

18. **Technology solutions and vendors.** Organisations implement technologies to enforce their policies and procedures. Organisations proactively acquire third-party services if necessary to augment their in-house CIRR capabilities. For instance, organisations invest in vulnerabilities detection software and automated patching solutions as part of their cyber resilience strategy. They implement commercially off-the-shelf technology solutions to protect systems from cyber threats. To reduce over dependence on a particular technology solution and vendor, organisations pursue a vendor and product diversification strategy.

19. **Third-party service providers**. Organisations maintain a record of third-party service agreements detailing important information such as the scope of the service, the service

provider contact information, service validity period and service levels. This is achieved through Service Level Agreements (SLAs) with Key Performance Indicators (KPIs), RPOs, and RTOs as part of the contract with the third-party service provider to guarantee adequate response during cyber incidents. Organisations look through SLAs that rely on subcontractors (e.g. n^{th} parties) and ensure they have protections in place. Organisations pre-designate a primary and an alternate service provider in the event that the former is unavailable to provide immediate support, especially in the case of a system-wide cyber incident. Organisations assess the service delivery capacity of their third-party service providers from the beginning and on an ongoing basis. This practice may prove useful in the case of a system-wide cyber incident where a service provider may not be able to conduct a service with sufficient capacity to support all its clients. Organisations monitor, manage and mitigate cyber risks stemming from third-party service providers through a variety of third-party risk management arrangements.

20. **Supply chain management.** Organisations manage dependencies in their supply chain and test the contingency measures. As supply chain risk covers a broad range of areas, organisations include cyber risks from third-party service providers or vendors, poor cyber security practices by suppliers, third-party data storage and software security vulnerabilities in their supply chain management or supplier systems. Organisations adopt supply chain risk management to ensure quality of the provided CIRR services.

3. Analysis

Organisations conduct analysis, including forensic analysis, and determine the severity, impact and root cause of cyber incidents to drive appropriate and effective CIRR activities.

21. **Cyber incident taxonomy.** Organisations use (i) a pre-defined taxonomy for classifying cyber incidents according to, for example, the type of incident, threat actors, threat vectors and repercussions; and (ii) a pre-established severity assessment framework that takes into consideration criticality of systems or services to help gauge the severity of the cyber incident. For example, an organisation may rely on indicators such as volume and types of network traffic to identify a DDoS attack. In addition to any applicable statutory or regulatory classifications, these taxonomies help organisations to prioritise and direct attention and resources to more timely and effective mitigation, restoration and recovery activities. Using a taxonomy will help establish consistency in the understanding of incidents across various parties, as information is communicated with a common language. Severity levels are established to allow for immediate response to a cyber incident as the first hours and few days following an incident are the most critical. This approach allows the execution of CIRR activities even in the absence of complete understanding of the incident.

Box 3: Examples of CIRR taxonomies

- Information used when describing cyber incidents
  - Describe the cause of the cyber incident (e.g. process failure, system failure, human error, external event, malicious action)
  - Describe whether the cyber incident due to a third-party service provider
  - Describe the attack vector (e.g. malware, virus, worm, malicious hyperlink)
  - Describe the delivery channel used (e.g. e-mail, web browser, removable storage media)
  - Describe the impact (e.g. service degradation/disruption, service downtime, potential impact to customers, data leakage, unavailability of data, data destruction/corruption, tarnishing of reputation)
  - Describe the type of incident (e.g. zero-day attack, exploiting a known vulnerability, isolated incident)
  - Describe the intent (e.g. malicious, theft, monetary gain, fraud, political, espionage, opportunistic)
  - Describe the threat actor (e.g. script kiddies, amateur, criminal syndicate, hacktivist, nation state)
- Classification of the severity of cyber incidents
  - Severity 1 incident has or will cause a serious disruption or degradation of critical systems or service(s) and there is potentially high impact on public confidence in the organisation.
  - Severity 2 incident has or will cause some degradation of critical services and there is medium impact on public confidence in the organisation.
  - Severity 3 incident little or no impact to critical systems or services and there is no visible impact on public confidence in the organisation.

22. **System and transaction logs.** Organisations retrieve the logs required for incident analysis and forensic investigation. Analysing the signs and indicators (e.g. from security alerts and system logs), investigating and correlating logs to identify the systems affected enables the response team to determine the impact of a cyber incident. The logs are stored and preserved in a secure and legally admissible manner. Organisations also retrieve data from relevant computing resources for analysing the cyber incident and possible actions. These data include lists of network-connected devices, running processes, users' sessions, open files, relevant configurations (e.g. network firewalls) and the contents of memory. The integrity of such data is continuously monitored.

23. **Trusted information sources.** Organisations correlate a variety of internal and external information sources for quick threat assessment and root cause analysis of the cyber incident.[15] For example, organisations join or subscribe to cyber threat intelligence sharing

[15] Examples of trusted sources are the multi-lateral information platforms.

sources (national/international CERT and sector information sharing platforms) to gather intelligence or recommendations on threats and on analysis of Tactics, Techniques, Procedures (TTPs)[16] and risk mitigation.

4. Mitigation

Organisations activate mitigation measures to prevent the aggravation of the situation and eradicate cyber incidents in a timely manner to alleviate their impact on business operations and services.

24. **Containment.** Organisations activate their containment measures and technologies best suited to each type of cyber incident to prevent the incident from inflicting further damage, including to connected entities. Having knowledge about what is the specific threat, such as Indicators of Compromise (IoCs),[17] and an understanding of its possible behaviours would also aid in the decision-making. Organisations monitor for anomalous activity and IoCs in connected, but apparently unaffected, networks and systems. Depending on the nature of the cyber incident, organisations make a claim on existing cyber insurance policies to alleviate the costs of recovery and help impact mitigation by obtaining relevant services offered by the policies, such as computer forensics, crisis management or public relations services.

25. **Business continuity measures.** Depending on the severity of a cyber incident, organisations invoke business continuity plans to maintain critical operations based on pre-defined prioritisation process. Examples of business continuity measures include activating contingency measures to facilitate the processing of critical transactions while system restoration efforts continue, or activating an alternative service provider if the primary service provider will not be able to recover from an incident within a certain period of time, as agreed in the respective SLA.

26. **Isolation.** Organisations consider the costs, business impact and operational risks when deciding whether to shut down or isolate all or substantial parts of their systems and networks, as opposed to maintaining their business services operations. Options for isolation include disconnecting the compromised systems from the network, adding network traffic blocking rules and obstructing threat actors' physical access to affected systems and networks.

27. **Eradication.** After evidence is collected and preserved, organisations remove all materials and artefacts (i.e. malicious code and data) introduced by the attacker. The process may involve patching and closing all system and network vulnerabilities that had been exploited by the attacker and validating the effectiveness of such counter measures. Organisations utilise antivirus and specialised tools to remove malware from the affected assets. Organisations also assess whether such measures are sufficient to address the particular

[16] FSB (2018), page 12.
[17] FSB (2018), page 10.

cyber incident and level of spread, or whether it is necessary to reinstall, replace or rebuild all compromised assets.

5. Restoration and recovery

Organisations restore systems or assets affected by a cyber incident to safely recover business-as-usual operations and delivery of impacted services.

28. **Prioritisation.** Organisations prioritise recovery activities based on the criticality of business operations, systems and supported services that drive security and restoration requirements. In order to classify the criticality of processes and systems, metrics like RTO and RPO or tiered criticality levels are used. All internal and external stakeholders are updated regularly and made aware of the conditions to be met or restrictions, before recovering critical operations.

29. **Data restoration.** Organisations restore data, including data maintained at third-party service providers, to meet business operations or service requirements. To provide assurance on data integrity (i.e. not been tampered or corrupted before restoration), organisations perform checks such as validating checksums and reconciliation to ensure data is consistent between systems when recovering from a cyber incident. To ensure data integrity, accessibility and readability, organisations perform on a regular basis data restoration tests at non-production environments.

30. **"Golden source" data.** Where appropriate, organisations restore backup data kept in another system, which is segregated (either physically or logically) from the main system and ensure that both systems are not directly connected. The "golden source" backup data are securely protected from unauthorised access or corruption.

31. **Approved restoration procedures.** Organisations carry out restoration activities based on documented and tested procedures. Where required, deviations from approved and tested procedures are assessed, tested and approved by management before implementation. This reduces the risk of human error that may arise in the manual, multistage restoration of systems and data. To restore affected systems, organisations use uncompromised system images and snapshots that are regularly updated, tested and securely stored to prevent malicious corruption or destruction.

32. **Key milestones.** Organisations define in CIRR plans key milestones to redesign, reinstall and reconfigure systems. Where it is not possible to achieve restoration of all systems, organisations consider defining interim restoration goals or interim measures, such as continuing operations in a diminished capacity instead of full capacity.

33. **Monitoring.** Organisations monitor third-party service providers, the network and systems for abnormal activities during the restoration process for compromised IT assets or for compromised third-party services to the extent possible. Recovery progress and resolutions are tracked and monitored, and updates are provided to management regularly. Organisations are responsible for their relationships with their third-party service providers and they establish SLAs that include prioritisation of service recovery plans, monitoring capabilities, and CIRR reporting in the event that the service provider cannot provide the

service or is providing it at a diminished capacity. Organisations adopt a wide range of monitoring capabilities suited for their size, complexity and risks.

34. **Validation.** Organisations validate that restored assets are free of compromise, fully functional and meet the security requirements before returning the systems to normal business operations for resumption of services.

35. **Record activities.** Organisations document and timestamp actions taken from the time the incident was detected to its final resolution. This record facilitates the tracing back of actions taken, reversing actions to reinstate to pre-incident conditions or troubleshooting should the recovery actions be unsuccessful. Tools and artefacts (e.g. scripts, configuration changes) used for recovery and restoration are recorded for future use or for the improvement of current processes and/or systems.

6. Coordination and communication

Across the life cycle of a cyber incident, organisations coordinate with their trusted stakeholders to maintain good cyber situational awareness and enhance the cyber resilience of the ecosystem in which they operate. During a cyber incident, organisations communicate on an agreed frequency, granularity and language appropriate to each stakeholder group, in order to engage and promote their CIRR activities. Close coordination with relevant internal and external stakeholders (see Box 2), including authorities, throughout the CIRR life cycle enables timely communication of progress and outcomes of the CIRR activities. Collective actions can be taken by stakeholders throughout their supply chain or orchestrated in their ecosystem.

36. **Timely escalation.** Organisations escalate cyber incidents to relevant stakeholders within the organisation based on the agreed severity assessment framework to avoid delays in addressing the incident. Timely escalation to the organisations' decision-makers is essential for the acceleration of CIRR actions, which include seeking approval and authorisation to implement response and recovery plans. Organisations also agree with third-party service providers to provide timely escalation wherever relevant through the SLAs. Organisations maintain the accuracy and integrity of information during this process and avoid hierarchical smoothing of risk as it traverses levels of seniority and functional or organisation boundaries.

37. **Cyber incident reporting.** Organisations report relevant information to the relevant authorities on cyber incidents as required by, and in accordance with, reporting timelines set by national requirements. In order to support effective and timely reporting of cyber incidents, organisations develop written internal guidelines that take into account the relevant legal and regulatory requirements for when and to whom an organisation needs to report different types and impacts of cyber incidents. These guidelines may include examples of different types of incidents and the types of reports to authorities in applicable jurisdictions that would be triggered by each incident type.

Box 4: Examples of information to be reported to authorities

- Date and time of discovery of the incident
- Time elapsed from detection to restoration of critical services
- Who discovered the incident (e.g. third-party service provider, customer, employee)
- Type and nature of cyber incident (e.g. DDoS, malware, intrusion/ unauthorised access, hardware/firmware failure, system software bugs)
- Impact of the incident (e.g. the financial and operational impact of the incident and implications on business continuity, loss of confidential information) and to which group of stakeholders
- Affected systems and technical details of the incident (e.g. source IP address and post, IoCs, TTPs)
- Escalation steps taken
- Decision(s) triaging, activation of business continuity or disaster recovery
- Other response and recovery activities taken to restore critical services
- Internal and external stakeholders informed or involved

38. **Regular updates with actionable messages.** Organisations inform relevant stakeholders about potential business disruptions caused by the cyber incident, the response and recovery activities taken and the plans to restore services. The information shared is actionable, accurate, timely, clear and relevant.[18] Both internal and external stakeholders are updated regularly at an appropriate frequency besides the urgent notifications as needed, and made aware of the conditions to be met or restrictions to be lifted before resuming critical services. Each message clearly states the actions that are expected to be taken by each audience. The frequency and intervals of such updates are set in advance to manage expectations.

39. **Media engagement.** Organisations engage the media using a pre-defined communications strategy and cross-functional communication team formed by representatives from functions such as affected business lines, human resources, press and communication offices, legal, technology and cyber security as well as the incident coordinator. Based on the incident type, the team may further enlist the assistance of other in-house specialists. To avoid confusion arising from information asymmetry, the media spokesperson consolidates relevant information and views from subject matter experts and the organisation's management to update the media with consistent information and message. Organisations make strategic use of communications channels such as conventional and social media.

40. **Cross-border coordination.** Organisations adopt the FSB *Cyber Lexicon* and other commonly used taxonomies from existing industry standards to facilitate effective coordination and exchange of information.

[18] *Actionable* refers to information that leads to implementation of concrete controls or configurations. *Accurate* refers to information that has, to the extent possible, been confirmed to be related to the cyber incident. Information is *timely* when it is distributed at a time when the recipient can take actions that minimise the impact of the incident.

41. **Trusted information sharing.** Organisations share information on significant cyber threat intelligence, cyber incidents, effective cyber security strategies and risk management practices through malware information sharing platforms. Technical information, such as IoCs or vulnerabilities exploited, are shared as soon as it is available with certain level of anonymity according to the confidentiality warranted.

Box 5: Examples of information to be shared with stakeholders

- A brief summary of the cyber threat or incident and lessons learnt
- Classification of information e.g. Traffic Light Protocol[19]
- Sources and key contact of the information provider
- Campaign, attack pattern investigated
- Exploited vulnerabilities already fixed or still emerging
- Threat actors or suspected attackers, if known, and root cause analysed
- Course of action already taken and planned
- Possible remedies and mitigations extracted from the precedent/ similar cases

42. **Trusted communication channels.** Organisations use trusted, secure communication channels over diversified architectures for redundancy to facilitate communication with relevant internal and external stakeholders, including authorities. Organisations and stakeholders regularly validate the availability of communication channels and regularly updated contacts list of relevant stakeholder groups.

7. Improvement

Organisations establish processes to improve CIRR activities and capabilities through lessons learnt from both proactive tools, such as CIRR exercises, tests and drills, and past cyber incidents. Lessons learnt are used in the selection and implementation of additional controls and mitigation measures, including changes to CIRR policies, plans and playbooks.

43. **Industry-wide initiatives**. Organisations collaborate with peers, such as in established forums, on sharing industry-wide knowledge, skill-sets, discussing cyber events and mitigation strategies against existing and potential cyber security vulnerabilities. Organisations also collaborate with authorities to promote information sharing and effective practices for the overall benefit of the industry. Their active engagement in trusted information sharing arrangements contributes to better mutual understanding of their key interdependencies in the financial system and enhances the organisation's capabilities to respond to and recover from cyber incidents.

44. **Post-incident analysis.** After the closure of a cyber incident, organisations analyse whether established procedures were followed and whether the actions taken were effective. This analysis may include: promptness in responding to security alerts; timeliness

[19] FSB (2018), page 13.

in determining the impact of incidents and incident severity; quality and speed in performing forensic analysis; effectiveness of incident escalation within the organisation; and effectiveness of communication (both internal and external).

45. **Exercises, tests and drills.** Organisations conduct tests on a regular basis, such as tabletop exercises and live simulations, to validate and improve the knowledge as well as understanding of resources regarding their CIRR activities and capabilities, and more in-depths drills to assess the robustness of their CIRR plans and procedures. In selecting the type of tests, organisations identify needs, goals (e.g. for developing skills, testing the effectiveness of plans, for "muscle memory") and – with regard to more invasive tests – any potential associated risks to measure their effectiveness. Organisations design their tests, depending on their size, complexity and risks, to incorporate interactions within the organisation as well as with external stakeholders and executive level decision-makers under simulated conditions. Organisations consider a wide range of different times (i.e. of the day, week, month or year) and occasions as inputs into the design of their exercises.

Box 6: Examples of scope and types of exercises, tests and drills

- Phishing exercises to test awareness and training of an organisation's employees.
- Tabletop exercises or drills/walk-throughs of CIRR plans or playbooks involving incident responders and incident management teams to build muscle memory.
- Live tests or simulations such as basic and threat-led penetration tests, bug bounty, cyber range and adversarial attack (DDoS, Ransomware) to enhance the actual technical response and recovery capabilities.
- Executive-level crisis management exercises to stress decision-making under simulated conditions, senior management involvement and communication proficiency. This could include developing challenging scenarios, such as dealing with no-win situations, uncertainty and imperfect information, or requiring the prioritisation of the timing of recovery of competing systems and business lines.
- Sector-wide exercises to allow financial sector participants practice CIRR coordination and communication in the event of a large-scale cyber incident.

46. **Cross-sectoral and cross-border exercises.** Organisations participate in cross-sectoral and cross-border crisis management and contingency exercises to prepare and enhance coordination among multiple stakeholders in the event of a cyber incident with systemic impact on the financial systems. These exercises include different scenarios to validate the effectiveness of coordination of the CIRR activities. Organisations are committed to overcoming challenges and impediments to the conduct of such exercises and sharing effective practices and lessons learnt with other participants, which include government and organisations. National authorities may participate in these exercises in the spirit of enhancing cyber resilience.

47. **Technological aids.** Organisations invest in the testing of the capabilities of CIRR systems by using a combination of technological aids. Automation tools, such as SOAR (Security Orchestration, Automation and Response), could help to improve CIRR processes. Organisations test tools in an isolated environment or non-production environment to validate the effectiveness of the tools to support CIRR activities.

48. **External events and sources.** Organisations identify opportunities for improvements to their CIRR activities from various sources: cyber publications; reports on cyber incidents; trend and threat analysis; regulatory and supervisory initiatives; changes to the environment, such as technological developments; and cyber risk management best practices.

49. **Lessons learnt.** Organisations validate lessons learnt with internal and external stakeholders, including business lines affected by the cyber incident, individuals with CIRR responsibilities and senior management. Organisations translate lessons learnt into remedial actions such as controls and procedures to improve future CIRR activities, and track these actions to closure. Closure includes revised metrics and incorporated procedures in plans, playbooks and training.

Conclusion

Enhancing cyber resilience requires a multifaceted approach comprising activities to support the Protect, Detect, Respond and Recover functions.[20] While organisations look to preventative capabilities to enhance their Protect and Detect functions, well-established response and recovery capabilities are essential to reduce the impact of a cyber incident and minimise the risk of contagion in the financial system.

This toolkit provides a set of effective practices that serve as building blocks for enhancing CIRR activities. Organisations can adopt and adapt from the range of practices in the toolkit to cater to the complexity of their IT environments and changing business models. Organisations and authorities alike will also evolve good practices in response to the changing cyber threat landscape, as they learn from their own experiences and gain additional insights from cyber incidents and near misses in terms of methods used and vulnerabilities exploited.

CIRR concerns all organisations in the financial ecosystem as the financial system is only as strong as its weakest link. Therefore, organisations and authorities must collectively strengthen their capabilities through frequent engagements in information sharing, exchange of best practices and cyber-related exercises.

[20] FSB (2018), pages 10 and 11 for definitions of the Protect and Detect functions.