Hong Kong Monetary Authority

<table>
<tr><th>Para</th><th>CIRR toolkit - suggested practices</th><th>Comments</th></tr>
<tr><td>General Comment</td><td colspan="2">Given the increasing integration and connectedness between financial institutions, technology and fintech service providers, we welcome the effective practices recommended for financial institutions' governance, risk management and continuous monitoring of third-party service providers. As cyber incidents may also happen to third-party service providers, it may be useful to enrich the effective practices by providing more guidance for financial institutions to cope with cyber incidents occurred in third parties (e.g. notification requirements and collaboration in incident response).</td></tr>
<tr><td>3</td><td>Roles, responsibilities and accountabilities for CIRR.
Organisations clearly define the roles, responsibilities and accountabilities for various CIRR activities to one or more named individuals that meet the pre-requisite role requirements. Potential conflicts of interest are minimised by ensuring a separation of implementation and oversight roles where possible. Apart from staff who are responsible for the various CIRR activities, organisations identify key roles (among others) to assist in managing the cyber incident. The roles are part of the multidisciplinary incident coordination team:
• Incident Owner: An individual is responsible for handling the overall CIRR activities according to the incident type and services affected. The Incident Owner is delegated appropriate authority to manage the mitigation of the incident. “Unity of command” is established by ensuring that incident responders report only to the Incident Owner for task assignment. The Incident Owner can minimise the potential
• Media Spokesperson: An individual is responsible for managing the communications strategy within a pre-determined cross-functional communication team, which may draw from areas such as affected business lines, human resources, press and communication offices, legal, technology and cyber security. Based on the incident type, the team may additionally 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. The Media Spokesperson is authorised to make strategic use of conventional and social media, fully consistent with the organisation’s official communication channels predefined in the Communication Plan.
• Scribe/Independent Observers: Organisations appoint individuals as independent observers to evaluate the effectiveness of CIRR activities during tests and actual incidents. These individuals are responsible for maintaining an accurate record of the cyber incident throughout its different 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.</td><td>The scope related to "Media Spokesperson" under para 3 could be broadened from "communication with media" to "communication with external stakeholders" such that other relevant parties (e.g. regulators, customers, etc.) could be also covered. Our experience indicates that it is very useful for financial institutions to have a dedicated party/function (e.g. compliance) who can explain clearly to the regulator the root cause of and mitigating measures for an incident as well as keep the regulator updated of the development. Such party/function may be different from those who are responsible for communicating with media.</td></tr>
</table>

Para	CIRR toolkit - suggested practices	Comments
6	**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.	A meaningful peer comparison is ideal and may be useful in identifying areas where funding should be channelled. However, there may be practical challenges to institutions in obtaining such information. It would be useful if the FSB could provide effective practices in this area.
14	**Disaster recovery sites.** Organisations replicate critical systems and data on a daily basis to disaster recovery sites and alternative sites (more often in case of business critical data). Backup facilities are diversified geographically and isolated through network and system segmentation to avoid possible concentration risks. In some cases, organisations choose to backup and store critical data in offline or air-gapped systems that effectively shield the data asset from unauthorised access. Organisations invest in (nearly) real-time mirroring to enhance the application recovery capability, appropriate (private) secured connections and integration with the primary facilities. Failover tests and recovery tests are performed regularly to validate effectiveness of these measures for ensuring availability and integrity of data and systems.	Para 14 mentions about air-gapped systems. As "air-gap" can be interpreted and implemented through various means (e.g. through logical or physical means) by different firms/vendors, it may be useful for FSB to further elaborate the definition of "air-gapped systems" such as by inserting a footnote, so as to make the implementation more practical. Besides failover tests and recovery tests, it is suggested that assessment/audits may also be conducted regularly to validate the effectiveness of the measures.

Para	CIRR toolkit - suggested practices	Comments
23	**Business continuity measures.** Organisations invoke business continuity plans during a cyber incident and resume critical operations based on pre-defined prioritisation process in the event restoration is expected to be protracted. Examples of business continuity measures include activating contingency measures not necessarily fully automated 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.	In resuming critical operations based on pre-defined prioritisation process, it would be useful for organisations to take into account their impact tolerance and own operational resilience requirements. The comment is based on our experiences from system/operational resilience perspective and the latest definition of Operational Resilience proposed by BCBS's Operational Resilience Group: "Operational resilience is defined as the ability of a bank to deliver critical operations through disruption. This ability would enable a bank to identify and protect itself from threats and potential failures, detect, respond and adapt to, recover and learn from, and minimise the impact of disruptive events in order to deliver critical operations through disruption, commensurate to their impact tolerance and own operational resilience requirements and taking into account their role in the financial system."
25	**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. Organisations utilise antivirus and specialised tools and software to remove malware from the affected assets. Organisations also assess whether such standard measures are sufficient to address the particular cyber incident and level of spread, or whether it is necessary to reinstall or rebuild all compromised assets.	For measures to be taken by organisations, apart from patching and removal of malware, it may be useful to also include cyber threat hunting (proactively searching through network to detect and isolate threats that evade existing security solutions).
32	**Data recovery.** Organisations recover and restore data, including data maintained at third-party service providers, to meet business 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. In worst-case scenario, organisations plan for the reconstruction of data from external stakeholders such as business partners and customers.	It may be useful to elaborate what is expected for the reconstruction of data from external stakeholders. It is unclear how to implement such plan in worst-case scenario which involve business partners and customers.

Para	CIRR toolkit - suggested practices	Comments
33	**“Golden source” data.** Where appropriate, organisations restore backup data kept in another system with a significantly different operating environment to 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.	Para 33 mentions about "data kept in another system with significantly different operating environment from the main system". As the current language "significantly different operating environment" could be interpreted differently by readers (e.g. Wintel vs. Mainframe, Oracle DB vs. MS SQL, Andriod vs. iOS, ... etc.), it may be useful for FSB to also consider other practices (e.g. Sheltered Harbor) and further elaborate the definition so as to allow sufficient flexibility and practical implementation. For example, "data kept in another system with significantly different operating environment from the main system" could be amended as "data kept in another system which is sufficiently (either physically or logically) segregated from the main system"
34	**Exercises, tests and drills.** Organisations conduct tests, such as tabletop exercises and live simulations, to validate the capability of resources and the robustness of their CIRR plans and procedures. Organisations design their tests to incorporate interactions within the organisation as well as with external stakeholders and executive level decision-makers under simulated conditions. The sophistication of these tests increases with the organisation’s cyber security maturity. Organisations set clear and appropriate objectives for tests and exercises (e.g. for developing skills, testing the effectiveness of plans, for “muscle memory”) to measure the effectiveness of the tests.	Para 34 mentions about exercises, tests and drills. It may be useful to specify that inputs could be obtained from the 2nd/3rd line of defence of the organisation to ensure adequacy of the tests.