Questions	Answers
Information about the respondent	
A. Name of respondent institution/firm	Singapore Exchange
B. Name of representative individual submitting response	Solomon Tay
C. Email address of representative individual submitting response	Solomon.Tay@sgx.com
D. Do you request non-publication of any part(s) of this response? If so, which part(s)? *Unless non-publication (in part or whole) is specifically requested, all consultation responses will be published in full on the FSB's website. An automated e-mail confidentiality claim will not suffice for these purposes.*	Information with specific references to SGX should be avoided.
E. Would you like your response to be confidential (i.e. not posted on the FSB website)?	No

Questions	Answers
Consultation questions	
General questions	
1. Have you learnt any lessons from the COVID-19 pandemic and related cyber activity that will contribute to your cyber incident response and recovery practices?	In Minimum Operating Requirements (MOR) planning, we find there is a shift of focus when moving from office to home, with consideration for concentration risks, as well as vulnerability of people to the spread of virus.
2. To whom do you think this document should be addressed within your organisation?	This document would be most appropriate to the Crisis Management Team.
3. How does your organisation link cyber incident response and recovery with the organisation's business? Does your organisation follow international standards or common frameworks? If so, which international standards or common frameworks?	SGX adopts the NIST and ISO27001 as part of our Cybersecurity Risk Assessment Framework, under the umbrella of the overall Enterprise Management Framework.
4. Does your organisation structure its cyber incident response and recovery activities along the seven components set out in the FSB toolkit? Please describe any additional components your organisation considers.	SGX broadly aligned to the 7 components in this FSB toolkit.
5. Based on your organisation's experience, please provide any additional effective practice(s) for any of the tools. Please list the number of the tool (e.g. Tools 1 – 46) and describe the effective practice(s).	The list of tools in this CIRR document is comprehensive, and therefore we do not have any additional practices to contribute beyond this list.
6. Based on your organisation's experience, please provide additional examples of effective practices listed in the boxes (e.g. Boxes 1-6).	The list of examples in this CIRR document is comprehensive, and therefore we do not have any additional examples to contribute beyond this list.

Questions	Answers
7. What role, if any, should authorities play in supporting an organisation's cyber incident response and recovery activities?	The authorities can play the role of "trusted party" that can facilitate the coordination of information exchange within the industry. For example, MAS / ABS to provide the communication to alert the FI community if one or more FIs are under attack.
1. Governance	
1.1 To what extent does your organisation designate roles and responsibilities as described in Tool 3? Does your organisation identify these roles by business line, technology application or department?	The roles within SGX are designed in accordance to the functional responsibilities performed by the staff.
1.2 How does your organisation promote a non-punitive culture to avoid "too little too late" failures and accelerate information sharing and CIRR activities?	SGX practice direct conversations between staff members through internal collaboration platforms (e.g. a number of internal chat groups are setup to allow for technical tracks as well as management tracks, besides the traditional voice conference bridges) so as to encourage timely sharing of information. This helps to create a safe environment for sharing and channel their efforts towards resolving the incident.
2. Preparation	
2.1 What tools and processes does your organisation have to deploy during the first days of a cyber incident?	As part of our major incident response procedure, we engage external responder to help with the forensic investigation during the onset of a cyber incident. The responder usually work closely with our internal investigation teams (SOC/CIRT) for triage of the incident using data from our SIEM to determine the extent of the impact and the root cause analysis.
2.2 Please provide an example of how your organisation has enhanced its cyber incident response plan over the last 12 months.	An example of how SGX has enhanced our cyber incident response plan – Conduct regular table-top drills on cyber related incidents for staff to ensure

Questions	Answers
	familiarity with the process and coordination between teams to improve the turnaround time during an incident.
2.3 How does your organisation monitor, manage and mitigate risks stemming from third-party service providers (supply chain)?	In terms of supply chain for SGX technology, we mainly focus in the areas of hardware and software provided by 3rd party to SGX. For software, we have existing stringent controls and measures to assess and mitigate risks through our various policies, procedures and processes. However, for hardware, many of the hardware products suppliers have multiple components (including CPU chips, memory chips, system board, network cards and etc) which the suppliers need to source from their own providers. This multi-tier relationship poses a challenge for SGX and therefore we rely heavily on our hardware supplier to ensure that they do the necessary quality assurance. We are also dependent on our hardware suppliers to apply the necessary international standards and processes to cover security tests to address the emerging risks on cyber threats related to their product sets. As such, we have a stringent process to evaluate vendors and hardware solutions based on the following areas: a) Goods specification and qualities – right fit for our purpose b) Reputation and financial strength of the vendor – continued vendor support and long term vision to ensure good security posture and long term commitment to ensure that their products maintain stringent security standards. c) Technical Competence and Support from vendor – ability of their support structure to ensure that there is up-to-date patches to ensure bugs or vulnerabilities are addressed timely.

Questions	Answers
	d) Past experiences with the vendor e) Price competitiveness of the product We use Gartner (Magic Quadrant) as well as other international companies such as Forrester Research in our research on assessment of IT Products. We also engage with independent analysts where necessary to seek their opinions for indepth assessments and comparisons against the best of breed products for a longer view of the vendor's roadmap. SGX also conduct reference checks with FI and major corporates using these product to solicit feedback for benchmarking. We limit the supplier and vendor base through a Preferred Vendor List. Vendor qualifies as a preferred vendor if they consistently provide high quality goods/ services at competitive prices, and has been approved by management. Preferred vendors are evaluated according to the points (a – e) mentioned above.
3. Analysis	
3.1 Could you share your organisation's cyber incident analysis taxonomy and severity framework?	Handling of cyber incidents is covered under SGX's major incident procedure where the severity levels are determined by the impact on financial, customer, service availability and regulatory compliance, and it is aligned with our incident management framework.
3.2 What are the inputs that would be required to facilitate the analysis of a cyber incident?	Usually the Indicators of Compromise (IOC), Indicators of Attack (IOA) as well as our SIEM logs are inputs required to facilitate the start of analysis. However, the investigation may also extend to system records and data set as part of the validation of compromise.
3.3 What additional tools could be useful to analyse the effectiveness of cyber incident response and recovery activities and the severity, impact and root cause of cyber incidents?	Besides conducting table-top exercises and having BCP drills that cover cyber scenarios for both IRT (incident response teams) and CMT (crisis management

Questions	Answers
	team), conducting Red teaming (adversarial simulation attacks) is also a good way to test the effectiveness of the response procedures and rec
3.4 What sector associations does your organisation participate in and what benefit does your organisations accrue from that participation?	As part of Singapore financial sector, we participate actively in the Association of Banks in Singapore (ABS), in the Standing Committee on Cyber Security (SCCS). This committee provides the platform for interaction and sharing of expertise on cybersecurity intelligence with the other major Financial Institutions (FI) and regulators (MAS/CSA) within Singapore. This allows SGX to be able to keep abreast of the emerging cyber threat landscape and adopt recommendations into our cyber strategy and workplan.
4. Mitigation	
4.1 Besides reducing impact to business and system security, what are other considerations that need to be taken into account during mitigation?	A possible consideration is to take up cyber insurance to cover financial losses or additional costs needed for recovery due to cyber attacks.
4.2 What tools or effective practices does your organisation have related to mitigating the impact from: (i) data breaches (ii) loss of data integrity and (iii) ransomware events?	Data Breaches – besides putting in a DLP systems with a comprehensive rule-set to detect and prevent data breaches, user education is also an important component to increase staff awareness on the implications of such breaches at the organisation level. Loss of Data integrity – as part of our system design, integrity checks are built within the application to detect and alert if data integrity is impacted by a cyber attack. Ransomware – having a rigourous system and data backup regime that helps to mitigate against ransomware attacks.
4.3 What tools or practices are effective for integrating the mitigation efforts of third-party service providers with the mitigation efforts of the organisation?	Our outsourcing governance committee oversees the framework for 3rd party engagement to ensure comprehensive risk assessment and mitigation controls are in place, and continuously reviewed on a regular basis.

Questions		Answers
4.4	What additional tools could be useful for including in the component Mitigation?	-
4.5	Are there situations in which effective practices for mitigation and restoration activities of the organisation are the same or overlap substantially? If yes, please provide examples.	-
5.	**Restoration**	
5.1	What tools and processes does your organisation have available for restoration?	In order to ensure that an impacted system can be restored effectively, SGX has internally developed a set of data recovery procedures that help to determine the area of impact and associated process flows to aid faster recovery time.
5.2	Which tools, plans, practices and metrics does your organisation use to prioritise restoration activities?	SGX uses system tiering to determine the priority of all activities, where higher priority is always given to our systems classified under Critical Information Infrastructure (CII) definition as well as their interconnected systems.
5.3	How does your organisation minimise undesirable outcomes of restoration activities, such as restoring affected data?	In our data recovery procedure, we determine the scope and integrity of affected data, before we determine the period of data restoration. This helps to minimise unnecessary and undesirable outcomes
6.	**Improvement**	
6.1	What are the most effective types of exercises, drills and tests? Why are they considered effective?	In SGX's context, having cross-functional participations from various fellow FI partners, members, regulators and staff with real life scenarios allows all the participants to relate to their past experiences. This allows them to identify gaps in their own respective areas and develop strategies and action plans to address these gaps. A good example would be the industry wide exercise, Ex Raffles that was held once every 2 years by ABS. In the 2019 exercise, there was involvement from >140+ FIs working together to respond against simulated real life cyber attacks across various FIs in Singapore.

Questions	Answers
6.2 What are the major impediments to establishing cross-sectoral and cross-border exercises?	In order to execute a well-coordinated exercise requires a great deal of planning and domain expertise, as well as commitment from the participating organisation's leadership. Having to align and ensure learning objectives are met across all participants can be complicated by a huge number of possible cyber threat scenarios faced by different sectors. Therefore such exercises would be best initiated by regulators or well-established associations (e.g. ABS) with strong support from its members to participate and contribute towards the planning of such activities.
6.3 Which technological aids and tools does your organisation consider most useful to improve cyber incident response and recovery?	Establishing a clear framework for cyber incident response is crucial towards the development of the strategies and procedures to tackle cyber incidents. It should lay down the principles of engagement between the involved parties and aid continuous improvement.
7. Coordination and Communication	
7.1 Does your organisation distinguish "coordination activities" from broader "communication" in general? If yes, please describe the distinct nature of each component.	With reference to cyber incidents, coordination activities usually refers to communication between teams within an organisation as part of the incident resolution process, and usually in the shortest possible timeframe to ensure all parties are in tandem. On the other hand, broader communication encompasses external parties such as regulators, partners and customers for updating of statuses or information, and these may be timed at deliberate intervals or milestones to serve the intent of regulating the flow of information.
7.2 How does your organisation address the possibility that email or traditional communication channels will be unavailable during a cyber incident?	While email may be one of the primary means of communication, SGX also uses conference bridges, chatgroups, SMS to deliver information across internal parties.

Questions	Answers
7.3 Apart from regulatory/compliance reporting, what other information does your organisation consider useful to share with authorities?	Sharing of threat intelligence and suspicious activities also helps the regulators to alert the FI community and be aware of potential attacks. SGX also shares information about cyber incidents from our members to our regulators as these may be relevant for learning about the attack patterns and be able to determine counter measures collectively as an industry.