## The Financial Stability Board (FSB) questions in consultative document for the toolkit in Cyber incident response and recovery (CIRR) activities

## Deadline for submission: 20 Jul 2020

Questions for each component	Tahoe Life Feedback
General	
1.1. 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?	Yes, as an organisation we learnt to be ever more vigilant as security incidents or pandemics can happen at any time and for prolonged periods. It is crucial that our cyber incident response and recovery practices need to be reviewed on a regular basis.
1.2. To whom do you think this document should be addressed within your organisation?	Risk teams, information security team, and senior management members.
1.3. 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?	<ul> <li>We have the security incident response team (SIRT) which links the organisation's business and other senior stakeholders.</li> <li>We follow the NIST cybersecurity framework and make reference to San Top 20 and ISO 27001.</li> </ul>
1.4. 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.	Yes, we do. Our cyber incident response and recovery is structured largely along the seven components.
1.5. 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).	We largely follow the listed number of tools, no additional.
1.6. Based on your organisation's experience, please provide additional examples of effective practices listed in the boxes (e.g. Boxes 1-6).	Nothing more to add to the six boxes.
1.7. What role, if any, should authorities play in supporting an organisation's cyber incident response and recovery activities?	More proactive to case and market intelligence sharing.
1.Governance	
1.1. To what extent does your organisation designate roles and responsibilities asdescribed in Tool 3? Does your organisation identify these roles by business line, technology application or department?	Yes, we do and similarly.
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?	We promote immediate security incident reporting in the organisation even with suspected cases. We have annual security awareness training for all staff and new joiners need to complete the mandatory e-course.
2. Preparation	
2.1. What tools and processes does your organisation have to deploy during the first days of a cyber incident?	We have implemented SIEM and have a dedicated team to analyse the security events.
2.2. Please provide an example of how your organisation has enhanced its cyber incident response plan over the last 12 months.	<ul> <li>We have adopted a number of tools to monitor the internal and external threat.</li> <li>In addition, we have regular security awareness training for all staff and regular security drill tests.</li> <li>Those exercises contribute and enhance our knowledge and response time.</li> </ul>
2.3. How does your organisation monitor, manage and mitigate risks stemming from third- party service providers (supply chain)?	Yes. We conduct third party security assesments prior to engaging vendors; and have regular performance meetings to gauge their performance and give proactive feedback.
3. Analysis	
3.1. Could you share your organisation's cyber incident analysis taxonomy and severity framework?	We classify by types of incident and severity level. Incident type: disruption of service, social engineering, APT, malicious attacks, unauthorised access, misuse, hoaxes, multiple components. Severity level: informational, low, medium, high.
3.2. What are the inputs that would be required to facilitate the analysis of a cyber incident?	The impact, source of incident, process involved, and affected tools and technology.

your organisations accrue from that participation? 4. Mitigation 4. Mitigation 4. Dissides reducing impact to business and system security, what are other consideration that need to be taken into account during mitigation? 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? 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? 4.4. What tools or practices are effective for integrating the mitigation? 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? 4.4. What additional tools could be useful for including in the component Mitigation? 4.4. What additional tools could be useful for including in the component Mitigation? 4.4. What additional tools could be useful for including in the component Mitigation? 5. Restoration 5. Restoration 5. Restoration 5. Which tools and processes does your organisation have available for restoration? 5. Restoration 5. Which tools, plans, practices and metrics does your organisation have available for restoration? 5. Which tools, plans, practices and metrics does your organisation have available for restoration? 5. Which tools, plans, practices and metrics does your organisation use to prioritise 5. Restoration 5. Which tools, plans, practices and metrics does your organisation use to prioritise 5. Restoration and the same trice wore yplan which documents clear responsibilities and priorities based on incident severity level. 5. Which tools and minimise undesirable outcomes of restoration activities 5. Allow does your organisation minimise undesirable outcomes of restoration activities 5. How does your organisation minimise undesirable outcomes of restoration activities 5. How does your organisation minimise	Questions for each component	Tahoe Life Feedback
response and recovery activities and the severity, impact and root cause of cyber incidents?       Our staff members join seminars organised by The Hong Kong Federation Insurers (HKFI) to enh our knowledge in all areas of insurance including cybersecurity.         3.4. What sector associations does your organisation participate in and what benefit does your organisations accrue from that participation?       Our staff members join seminars organised by The Hong Kong Federation Insurers (HKFI) to enh our knowledge in all areas of insurance including cybersecurity.         4.1. Betides reducing impact to business and system security, what are other consideration that need to be taken into account during mitigation?       Our communication with the regulator for continuus feedback.         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?       Tools include: - FortiMail Email Security Appliance - Inslights Threat Intelligent Platform - Symmate Endpoint and TrendMicro Deep Security Effective practices being: Internal policies and standards, SIEM, latest anti-virus tools & others, a incldent reporting process.         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?       We use the following tools for managing the third party - Security risk assessment - SLA At the same time, we have the CITIC as the SOC and ATOS as our Data center to manage inciden monitor the security services.         5. Are there situations in which effective practices for mitigation and restoration?       The suggested list is quite comprehensive, nothing more to add. <tr< td=""><td></td><td></td></tr<>		
your granisations accrue from that participation?         our knowledge in all areas of insurance including cybersecurity.           4. Mitigation         4. Besides reducing impact to business and system security, what are other considerations         Our communication with the regulator for continous feedback.           4.1. Besides reducing impact to business and system security, what are other considerations         Our communication with the regulator for continous feedback.           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?         Tools include: - IntSights Threat Intelligent Platform           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?         We use the following tools for managing the third party           -Security risk seasement         -SUA           4.4. What additional tools could be useful for including in the component Mitigation?         The suggested list is quite comprehensive, nothing more to add.           4.5. Are there situations in which effective practices for mitigation and restoration activities         No overlap.           5.1. What tools and processes does your organisation have available for restoration?         Back-up technology solutions, disaster recovery site, etc.           5.2. Which tools plans, practices and entrics does your organisation use to priorities restoration?         Back-up technology solutions, disaster recovery site, etc.		
your organisations accrue from that participation?         our knowledge in all areas of insurance including cybersecurity.           4. Mitigation         4.1. Besides reducing impact to business and system security, what are other considerations         Our communication with the regulator for continous feedback.           4.1. Besides reducing impact to business and system security, what are other considerations         Our communication with the regulator for continous feedback.           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?         Tools include:           - IntSights Threat Intelligent Platform         - Symmatic Endopin and TrendMicro Deep Security           4.3. What tools or practices are effective for integrating the mitigation efforts of third-party         Yee use the following tools for managing the third party           -Security risk assessment         - SQA           -SQA         At the same time, we have the CITIC as the SOC and ATOS as our Data center to manage inciden monitor the security services.           4.4. What additional tools could be useful for including in the component Mitigation?         The suggested list is quite comprehensive, nothing more to add.           4.5. Are three situations in which effective practices for mitigation and restoration activities         No overlap.           5.1. What tools and processes does your organisation have available for restoration?         Back-up technology solutions, disaster recovery site, etc. <t< td=""><td>3.4. What sector associations does your organisation participate in and what benefit does</td><td>Our staff members join seminars organised by The Hong Kong Federation Insurers (HKFI) to enhance</td></t<>	3.4. What sector associations does your organisation participate in and what benefit does	Our staff members join seminars organised by The Hong Kong Federation Insurers (HKFI) to enhance
4. Mitgation		
4.1. Besides reducing impact to business and system security, what are other considerations.       Our communication with the regulator for continuus feedback.         Another key considerations is the restoration of the business as soon as possible and reduce the reputation risk towards the customers.         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?       Tools include:         - Insights Threat Intelligent Platform       - Symantce Endpoint and TrendMicro Deep Security         Effective practices are effective for integrating the mitigation efforts of third-party       Effective practices being: Internal policies and standards, SIEM, latest anti-virus tools & others, a incident reporting process.         4.3. What tools or practices are effective for integrating the mitigation efforts of third-party       Yee use the following tools for managing the third party         -security risk assessment       -SIA         -SIA       At the same time, we have the CITIC as the SOC and ATOS as our Data center to manage inciden monitor the security services.         4.4. What additional tools could be useful for including in the component Mitigation?       The suggested list is quite comprehensive, nothing more to add.         5. Restoration       S. Restoration       So recervices and metrics does your organisation have available for restoration?         5.1. What tools and processes does your organisation bas to prioritise restoration activities?       Disaster recovery plan which documents clear res		
that need to be taken into account during mitigation?       Another key consideration is the restoration of the business as soon as possible and reduce the reputation risk towards the customers.         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?       Tools include: -FortiMail Email Security Appliance - IntSights Threat Intelligent Platform - Symantec Endpoint and TrendMicro Deep Security         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?       We use the following tools for managing the third party - Security risk assessment - Security risk assessment - Security risk assessment - Security services.         4.4. What additional tools could be useful for including in the component Mitigation and restoration activities?       The suggested list is quite comprehensive, nothing more to add.         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.       No overlap.         5. Restoration       Situct tools, plane, practices and metrics does your organisation use to prioritise testoration activities?       Disaster recovery plan which documents clear responsibilities and priorities based on incident severity level.         5.3. How does your organisation minimise undesirable outcomes of restoration activities on the severity rating.       Disaster recovery plan which documents dear responsibilities and priorities based on incident severity rating.	-	Our communication with the regulator for continous feedback.
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?       Tools include: <ul> <li>-fortiMail Email Security Appliance</li> <li>-Instights Thread Intelligent Platform</li> <li>-Symantee Endpoint and TrendMicro Deep Security</li> </ul> 4.3. What tools or practices are effective for integrating the mitigation efforts of third-party         Security risk assessment <li>-Such and tools could be useful for including in the component Mitigation?</li> <li>-A. What additional tools could be useful for including in the component Mitigation?</li> <li>-A. The there situations in which effective practices for mitigation and restoration activities of the organisation have available for restoration?</li> <li>-S. Restoration</li> <li>-S. Which tools, plans, practices and metrics does your organisation use to prioritise restoration activities?</li> <li>-S. Which tools, plans, practices and metrics does your organisation use to prioritise restoration activities?</li> <li>-S. Which tools and processes does your organisation have available for restoration activities on the maker and checker process which requires data domain owner sign-off. Prior to that, this the maker and checker process which requires data domain owner sign-off. Prior to that, this the maker and checker process which requires data domain owner sign-off. Prior to that, this the maker and checker process which induition, incidents are prioritise base on the severity rating.</li>		
impact from: (i) data breaches (ii) loss of data integrity and (iii) ransomware events?       - FortiMail Email Security Appliance         - IntSights Threat Intelligent Platform       - Symantec Endpoint and TrendMicro Deep Security         Effective practices are effective for integrating the mitigation efforts of third-party       Effective practices being: Internal policies and standards, SIEM, latest anti-virus tools & others, a incident reporting process.         4.3. What tools or practices are effective for integrating the mitigation efforts of the organisation?       We use the following tools for managing the third party         service providers with the mitigation efforts of the organisation?       -Security risk assessment         -SLA       -SLA         4.4. What additional tools could be useful for including in the component Mitigation?       The suggested list is quite comprehensive, nothing more to add.         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.       No overlap.         5. Restoration		
<ul> <li>IntSights Threat Intelligent Platform</li> <li>Symantec Endpoint and TrendMicro Deep Security</li> <li>Effective practices being: Internal policies and standards, SIEM, latest anti-virus tools &amp; others, a incident reporting process.</li> <li>4.3. What tools or practices are effective for integrating the mitigation efforts of third-party</li> <li>Service providers with the mitigation efforts of the organisation?</li> <li>Security risk assessment</li> <li>SLA</li> <li>At the same time, we have the CITIC as the SOC and ATOS as our Data center to manage inciden monitor the security services.</li> <li>4.4. What additional tools could be useful for including in the component Mitigation?</li> <li>The suggested list is quite comprehensive, nothing more to add.</li> <li>At the same time, we have the CITIC as the SOC and ATOS as our Data center to manage inciden monitor the security services.</li> <li>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.</li> <li>S. Restoration</li> <li>S. Which tools, plans, practices and metrics does your organisation use to prioritise restoration activities?</li> <li>S. How does your organisation minimise undesirable outcomes of restoration activities, such as restoring affected data?</li> <li>Me have clear documented process which requires data domain owner sign-off. Prior to that, the sum are and checker process with authorised staff. In addition, incidents are prioritise based on the severity rating.</li> </ul>	4.2. What tools or effective practices does your organisation have related to mitigating the	Tools include:
- IntSights Threat Intelligent Platform     - Symantec Endpoint and TrendMicro Deep Security     Effective practices being: Internal policies and standards, SIEM, latest anti-virus tools & others, a     incident reporting process.     4.3. What tools or practices are effective for integrating the mitigation efforts of third-party     We use the following tools for managing the third party     -Security risk assessment     -SLA     A the same time, we have the CITIC as the SOC and ATOS as our Data center to manage inciden     monitor the security services.     4.4. What additional tools could be useful for including in the component Mitigation?     The suggested list is quite comprehensive, nothing more to add.     S. 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.     S. Restoration     S. What tools and processes does your organisation have available for restoration?     S. Which tools, plans, practices and metrics does your organisation use to prioritise     restoration activities?     S. Alwo does your organisation minimise undesirable outcomes of restoration activities,     such as restoring affected data?     Me have clear documented process which requires data domain owner sign-off. Prior to that, th     is the maker and checker process with authorised staff. In addition, incidents are prioritise base     on the severity rating.		- FortiMail Email Security Appliance
<ul> <li>- Symantec Endpoint and TrendMicro Deep Security</li> <li>Effective practices being: Internal policies and standards, SIEM, latest anti-virus tools &amp; others, a incident reporting process.</li> <li>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?</li> <li>Security risk assessment -Regular Vendor assessment -SLA At the same time, we have the CITIC as the SOC and ATOS as our Data center to manage inciden monitor the security services.</li> <li>4.4. What additional tools could be useful for including in the component Mitigation?</li> <li>The suggested list is quite comprehensive, nothing more to add.</li> <li>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.</li> <li>S. Restoration</li> <li>S. Restoration</li> <li>S. What tools and processes does your organisation have available for restoration?</li> <li>Back-up technology solutions, disaster recovery site, etc.</li> <li>S. Whot cools and metrics does your organisation use to prioritise restoration activities?</li> <li>S. How does your organisation minimise undesirable outcomes of restoration activities, such as restoring affected data?</li> <li>Me have clear documented process which requires data domain owner sign-off. Prior to that, th is the maker and checker process with authorised staff. In addition, incidents are priorities base on the severity rating.</li> </ul>		- IntSights Threat Intelligent Platform
incident reporting process.         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?       We use the following tools for managing the third party -Security risk assessment -Regular Vendor assessment -SLA         4.4. What additional tools could be useful for including in the component Mitigation?       The suggested list is quite comprehensive, nothing more to add.         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.       No overlap.         5. Restoration       S.         5.1. What tools and processes does your organisation have available for restoration?       Back-up technology solutions, disaster recovery site, etc.         5.2. Which tools, plans, practices and metrics does your organisation use to prioritise restoration activities?       Disaster recovery plan which documents clear responsibilities and priorities based on incident severity level.         5.3. How does your organisation minimise undesirable outcomes of restoration activities, such as restoring affected data?       We have clear documented process which requires data domain owner sign-off. Prior to that, th is the maker and checker process with authorised staff. In addition, incidents are prioritise base on the severity rating.         6. Improvement       Improvement		
4.3. What tools or practices are effective for integrating the mitigation efforts of third-party       We use the following tools for managing the third party         service providers with the mitigation efforts of the organisation?       -Security risk assessment         -Regular Vendor assessment       -SLA         4.4. What additional tools could be useful for including in the component Mitigation?       The suggested list is quite comprehensive, nothing more to add.         4.5. Are there situations in which effective practices for mitigation and restoration activities       No overlap.         of the organisation are the same or overlap substantially? If yes, please provide examples.       No overlap.         5. Restoration       Security risk not be providers which documents clear responsibilities and priorities based on incident severity level.         5.2. What tools, plans, practices and metrics does your organisation use to prioritise restoration activities?       Disaster recovery plan which documents clear responsibilities and priorities based on incident severity level.         5.3. How does your organisation minimise undesirable outcomes of restoration activities?       We have clear documented process which requires data domain owner sign-off. Prior to that, th is the maker and checker process which undurinsed staff. In addition, incidents are prioritise based on the severity rating.         6. Improvement       Improvement		Effective practices being: Internal policies and standards, SIEM, latest anti-virus tools & others, and incident reporting process
service providers with the mitigation efforts of the organisation?       -Security risk assessment         -SLA       -SLA         At the same time, we have the CITIC as the SOC and ATOS as our Data center to manage inciden monitor the security services.         4.4. What additional tools could be useful for including in the component Mitigation?       The suggested list is quite comprehensive, nothing more to add.         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.       No overlap.         5. Restoration       5.1. What tools and processes does your organisation have available for restoration?       Back-up technology solutions, disaster recovery site, etc.         5.2. Which tools, plans, practices and metrics does your organisation use to prioritise restoration activities?       Disaster recovery plan which documents clear responsibilities and priorities based on incident severity level.         5.3. How does your organisation minimise undesirable outcomes of restoration activities, such as restoring affected data?       We have clear documented process which requires data domain owner sign-off. Prior to that, th is the maker and checker process with authorised staff. In addition, incidents are prioritise on the severity rating.         6. Improvement       Improvement	13 What tools or practices are effective for integrating the mitigation efforts of third parts	
-Regular Vendor assessment         -SLA         At the same time, we have the CITIC as the SOC and ATOS as our Data center to manage inciden monitor the security services.         4.4. What additional tools could be useful for including in the component Mitigation?       The suggested list is quite comprehensive, nothing more to add.         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.       No overlap.         5. Restoration       5.1. What tools and processes does your organisation have available for restoration?       Back-up technology solutions, disaster recovery site, etc.         5.2. Which tools, plans, practices and metrics does your organisation use to prioritise restoration activities?       Disaster recovery plan which documents clear responsibilities and priorities based on incident severity level.         5.3. How does your organisation minimise undesirable outcomes of restoration activities, such as restoring affected data?       We have clear documented process which requires data domain owner sign-off. Prior to that, the is the maker and checker process with authorised staff. In addition, incidents are prioritise data on the severity rating.         6. Improvement       4		
-SLA         At the same time, we have the CITIC as the SOC and ATOS as our Data center to manage inciden monitor the security services.         4.4. What additional tools could be useful for including in the component Mitigation?       The suggested list is quite comprehensive, nothing more to add.         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.       No overlap.         5. Restoration       5.1. What tools and processes does your organisation have available for restoration?       Back-up technology solutions, disaster recovery site, etc.         5.2. Which tools, plans, practices and metrics does your organisation use to prioritise restoration activities?       Disaster recovery plan which documents clear responsibilities and priorities based on incident severity level.         5.3. How does your organisation minimise undesirable outcomes of restoration activities, such as restoring affected data?       We have clear documented process with authorised staff. In addition, incidents are prioritise data on the severity rating.         6. Improvement       1	ervice providers with the initigation eriors of the organisation:	
At the same time, we have the CITIC as the SOC and ATOS as our Data center to manage inciden monitor the security services.         4.4. What additional tools could be useful for including in the component Mitigation?       The suggested list is quite comprehensive, nothing more to add.         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.       No overlap.         5. Restoration       5. Restoration         5.1. What tools and processes does your organisation have available for restoration?       Back-up technology solutions, disaster recovery site, etc.         5.2. Which tools, plans, practices and metrics does your organisation use to prioritise restoration activities?       Disaster recovery plan which documents clear responsibilities and priorities based on incident severity level.         5.3. How does your organisation minimise undesirable outcomes of restoration activities, such as restoring affected data?       We have clear documented process which requires data domain owner sign-off. Prior to that, th is the maker and checker process with authorised staff. In addition, incidents are prioritise base on the severity rating.         6. Improvement       Improvement		-
4.4. What additional tools could be useful for including in the component Mitigation?       The suggested list is quite comprehensive, nothing more to add.         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.       No overlap.         5. Restoration       5.         5.1. What tools and processes does your organisation have available for restoration?       Back-up technology solutions, disaster recovery site, etc.         5.2. Which tools, plans, practices and metrics does your organisation use to prioritise restoration activities?       Disaster recovery plan which documents clear responsibilities and priorities based on incident severity level.         5.3. How does your organisation minimise undesirable outcomes of restoration activities, such as restoring affected data?       We have clear documented process which requires data domain owner sign-off. Prior to that, th is the maker and checker process with authorised staff. In addition, incidents are prioritised base on the severity rating.         6. Improvement       Everity rating.		
<ul> <li>4.4. What additional tools could be useful for including in the component Mitigation?</li> <li>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.</li> <li>5. Restoration</li> <li>5. Restoration</li> <li>5.1. What tools and processes does your organisation have available for restoration?</li> <li>5.2. Which tools, plans, practices and metrics does your organisation use to prioritise restoration activities?</li> <li>5.3. How does your organisation minimise undesirable outcomes of restoration activities, such as restoring affected data?</li> <li>6. Improvement</li> </ul>		-
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.       No overlap.         5. Restoration       5. Restoration         5.1. What tools and processes does your organisation have available for restoration?       Back-up technology solutions, disaster recovery site, etc.         5.2. Which tools, plans, practices and metrics does your organisation use to prioritise restoration activities?       Disaster recovery plan which documents clear responsibilities and priorities based on incident severity level.         5.3. How does your organisation minimise undesirable outcomes of restoration activities, such as restoring affected data?       We have clear documented process which requires data domain owner sign-off. Prior to that, th is the maker and checker process with authorised staff. In addition, incidents are prioritised bas on the severity rating.         6. Improvement       External data		monitor the security services.
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?       Back-up technology solutions, disaster recovery site, etc.         5.2. Which tools, plans, practices and metrics does your organisation use to prioritise restoration activities?       Disaster recovery plan which documents clear responsibilities and priorities based on incident severity level.         5.3. How does your organisation minimise undesirable outcomes of restoration activities, such as restoring affected data?       We have clear documented process which requires data domain owner sign-off. Prior to that, th is the maker and checker process with authorised staff. In addition, incidents are prioritised bas on the severity rating.         6. Improvement       Everity rating.	4.4. What additional tools could be useful for including in the component Mitigation?	The suggested list is quite comprehensive, nothing more to add.
5.1. What tools and processes does your organisation have available for restoration?       Back-up technology solutions, disaster recovery site, etc.         5.2. Which tools, plans, practices and metrics does your organisation use to prioritise restoration activities?       Disaster recovery plan which documents clear responsibilities and priorities based on incident severity level.         5.3. How does your organisation minimise undesirable outcomes of restoration activities, such as restoring affected data?       We have clear documented process which requires data domain owner sign-off. Prior to that, the is the maker and checker process with authorised staff. In addition, incidents are prioritised bas on the severity rating.         6. Improvement       Execution activities		No overlap.
5.2. Which tools, plans, practices and metrics does your organisation use to prioritise restoration activities?       Disaster recovery plan which documents clear responsibilities and priorities based on incident severity level.         5.3. How does your organisation minimise undesirable outcomes of restoration activities, such as restoring affected data?       We have clear documented process which requires data domain owner sign-off. Prior to that, the is the maker and checker process with authorised staff. In addition, incidents are prioritised based on the severity rating.         6. Improvement       Improvement	5. Restoration	
restoration activities?       severity level.         5.3. How does your organisation minimise undesirable outcomes of restoration activities, such as restoring affected data?       We have clear documented process which requires data domain owner sign-off. Prior to that, the is the maker and checker process with authorised staff. In addition, incidents are prioritised bas on the severity rating.         6. Improvement       Example 1	5.1. What tools and processes does your organisation have available for restoration?	Back-up technology solutions, disaster recovery site, etc.
<ul> <li>5.3. How does your organisation minimise undesirable outcomes of restoration activities, such as restoring affected data?</li> <li>6. Improvement</li> </ul> We have clear documented process which requires data domain owner sign-off. Prior to that, the maker and checker process with authorised staff. In addition, incidents are prioritised bas on the severity rating.	5.2. Which tools, plans, practices and metrics does your organisation use to prioritise	Disaster recovery plan which documents clear responsibilities and priorities based on incident
such as restoring affected data?       is the maker and checker process with authorised staff. In addition, incidents are prioritised bas on the severity rating.         6. Improvement       is the maker and checker process with authorised staff. In addition, incidents are prioritised bas on the severity rating.	estoration activities?	severity level.
on the severity rating. 6. Improvement	5.3. How does your organisation minimise undesirable outcomes of restoration activities,	We have clear documented process which requires data domain owner sign-off. Prior to that, there
6. Improvement	such as restoring affected data?	is the maker and checker process with authorised staff. In addition, incidents are prioritised based
		on the severity rating.
6.1. What are the most effective types of exercises, drills and tests? Why are they Both are very effective.	j. Improvement	
	5.1. What are the most effective types of exercises, drills and tests? Why are they	Both are very effective.
considered effective?	considered effective?	
6.2. What are the major impediments to establishing cross-sectoral and cross-border Trust, legal and different nature of business.	5.2. What are the major impediments to establishing cross-sectoral and cross-border	Trust, legal and different nature of business.
exercises?	exercises?	
6.3. Which technological aids and tools does your organisation consider most useful to Artificial intelligence (AI) technology tools would help to automate the response process.	5.3. Which technological aids and tools does your organisation consider most useful to	Artificial intelligence (AI) technology tools would help to automate the response process.
improve cyber incident response and recovery?		
7. Coordination and communication		
7.1. Does your organisation distinguish "coordination activities" from broader No, we do not, all are part of the list of activities.		No, we do not, all are part of the list of activities.
"communication" in general? If yes, please describe the distinct nature of each component.		
7.2. How does your organisation address the possibility that email or traditional We have established the call tree and also regular call tree exercise to ensure the communication	.2. How does your organisation address the possibility that email or traditional	We have established the call tree and also regular call tree exercise to ensure the communication
	communication channels will be unavailable during a cyber incident?	-
Other consideration includes WeChat.		
7.3. Apart from regulatory/compliance reporting, what other information does your What's covered is quite comprehensive, no more to add.		what's covered is quite comprehensive, no more to add.
organisation consider useful to share with authorities?		