RESPONSES TO FEEDBACK RECEIVED

CYBERSECURITY CODE OF PRACTICE FOR CRITICAL INFORMATION INFRASTRUCTURE - SECOND EDITION

JULY 2022

CONTENTS

1 PREFACE

1.1. On 28 February 2022, the Cyber Security Agency of Singapore ("CSA") issued the draft Cybersecurity Code-of-Practice – Second Edition ("CCoP 2.0") to all Sector Leads and CII Owners ("CIIOs") to seek feedback.

1.2. The CCoP 2.0 seeks to level up new cybersecurity capabilities in the Critical Information Infrastructure ("CII") sectors due to the following impetus:

(a) the cyber threat landscape has evolved with threat actors using sophisticated tactics, techniques and procedures ("TTPs") to attack CII sectors;

(b) each CII sector faces cybersecurity risks that are specific to their digital terrain; and

(c) cyber-attacks have increased in scale and sophistication to a point where they could present systemic risks to Singapore.

1.3. The CCoP 2.0 aims to:

(a) improve the odds of defenders against threat actors sophisticated TTPs and impede their progress of attacks;

(b) enhance agility in addressing emerging risks in specific domains (e.g. Cloud, 5G, AI); and

(c) enable coordinated defenses between Government and Private sectors to identify, discover and respond to cybersecurity threats and attacks on a timely basis.

1.4. The feedback was solicited from Sector Leads, CIIOs, industry and trade associations. CSA has reviewed all feedback and effected changes to the CCoP 2.0, where appropriate.

1.5. CSA would like to thank all respondents for their contributions.

2 GENERAL COMMENTS

SCOPE OF CCOP

Feedback

2.1. Respondents sought clarification on whether CCoP 2.0 is scoped only for the CII system or is also to be extended to cover the entire CII organisation.

CSA's Response

2.2. The CCoP 2.0 is applicable to the CII systems. The CII system includes computer systems, network components, and end-point devices within the digital boundary defined jointly between CSA, CIIOs, and their Sector Leads.

2.3. However, the CIIO should consider extending some cybersecurity capabilities to the entire CII organisation because many of these capabilities are also relevant to strengthening the cybersecurity posture of the entire CII organisation. The cybersecurity capabilities can be found under Annex A of CCoP 2.0. The cybersecurity capabilities under Annex A of CCoP 2.0 is not to be included in the scope for the cybersecurity audit under the Cybersecurity Act.

AUDIT REFERENCE

Feedback

2.4. Respondents sought clarification on the audit scope reference applicable for the 2022 cybersecurity audit cycle mandated to be performed under the Cybersecurity Act.

CSA's Response

2.5. CCoP 2.0 will only come into compliance 12 months after the issuance of CCoP 2.0. Cybersecurity Code-of-Practice – First Edition will only be applicable to the cybersecurity audit conducted with audit period that falls before the compliance date of CCoP 2.0. Thereafter, CCoP 2.0 must be used for subsequent audits. However, the CIIO may use CCoP2.0 for their audit before the compliance date if they are ready.

2.6. Additionally, the CIIO need to ensure the following requirements are adhered to with respect to the conduct of the CII cybersecurity audit:

(a) there must be no gaps in the audit period between the previously completed cybersecurity audit and the to-be-completed cybersecurity audit; and

(b) the audit period must be at least 12 months.

HARMONISATION OF CCOP 2.0 WITH INSTRUCTION MANUAL 8

Feedback

2.7. Respondents highlighted that there are overlaps in requirements on access control management, and system hardening between Government's Instruction Manual 8 ("IM8") and CCoP 2.0.

2.8. Respondents also raised concerns on the resources needed to conduct two audits to fulfil IM8 and CCoP 2.0 requirements.

CSA's Response

2.9. CSA noted that the national code of practice ("CCoP") may at times overlap with the sectoral cybersecurity requirements. Under such circumstances, harmonisation of codes will be carried out to:

(a) deconflict requirements; and

(b) to allow an audit that is mutually recognised under the Cybersecurity Act and IM8 requirements.

COMPLIANCE TIMELINE

Feedback

2.10. Respondents sought clarification on the compliance timeline for each clause and the short grace period given to implement the new requirements for the Operational Technology ("OT") environment.

CSA's Response

2.11. The compliance timeline in the initial CCoP 2.0 draft was with immediate effect for existing clauses, 30 days grace period for clauses formalised from COI and PSDSRC recommendations and 9 months grace period for new clauses. However, CSA has revised the compliance timeline to a grace period of 12 months for all clauses for the compliance of CCoP 2.0. This will apply to both existing and any newly designated CII.

2.12. CSA recognised the technical and/or operational challenges to implement the revised heightened cybersecurity requirements and the need for longer grace period to comply with all the requirements. Unfortunately, the impending cybersecurity threats have raised the need for more effective measures to be built-up expediently to reduce cybersecurity risks. Cybersecurity is a continuous process of risk reduction.

2.13. The Act does not penalise a CIIO that required more time and/or resources to implement the measures. It allows the Commissioner to grant the necessary waivers when there are valid reasons. If the CIIO is unable to comply with any specific CCoP 2.0 requirements, it may submit a request of waiver made available under Section 11(7) of the Cybersecurity Act to the Commissioner. The Commissioner has the authority to reject the waiver if the mitigating or compensating controls are deemed to be insufficient.

RECURRING REQUIREMENTS

Feedback

2.14. Respondents sought clarification on the deadline for recurring requirements (e.g. a requirement to perform an act at least once every 12 months) after the CCoP 2.0 comes into effect.

CSA's Response

2.15. For Existing CII, the deadline of the recurring requirements will be based on the date that the previous instance was performed, even if the instance was performed when the previous version of CCoP is still in effect.

2.16. For Redesignated CII, the deadline of the recurring requirements will be based on the date the previous instance was performed, even if the instance was performed during the previous designation period.

WAIVER

Feedback

2.17. Respondents sought clarification on the submission timeline for waiver request and that are not implementable or not applicable to the CII.

CSA's Response

2.18. The CIIO should submit a waiver from compliance with any clause in the Cybersecurity Act, applicable codes of practice and standards of performance as soon as the CIIO has completed its assessment and determined that it is unable to comply with a specific clause requirement.

2.19. Technology, operating terrains, and their associated threats evolved from time to time. Permanent wavier will not be granted even when the risks are not applicable during the time of assessment. A time bound wavier compels CIIO to evaluate changes to ensure that cyber risks are monitored and pre-emptively mitigated to an acceptable level.

2.20. The CIIO is not required to submit a waiver request for any clause that is not applicable to the CII.

Feedback

2.21. Respondents enquired on the time expected for a waiver request to be reviewed and processed, and if the CIIO is expected to carry out any actions while the waiver request is being reviewed.

CSA's Response

2.22. A CIIO can typically expect to hear back on the status of their waiver request within 4 weeks upon the submission of all relevant supporting documents. However, the expected time frame may vary as each waiver request is subjected to the completeness of the submission and the complexity of the case. The CIIO can follow up with the respective CSA sector officers on the status of the waiver request.

2.23. During the review period of the waiver, the CIIO is expected to continue to monitor the risks associated with the CCoP clause which could not be complied with and to ensure that the compensating controls are implemented to reduce the cybersecurity risks.

DEFINITION

Feedback

2.24. Respondents requested for definitions to the terms used in CCoP 2.0 such as "raw logs" and "baseline of normal operations" to avoid misinterpretation of the clauses.

CSA's Response

2.25. The glossary and interpretation section in CCoP 2.0 has been updated with the definition and explained the terminology of new words used in the clauses. The CIIO should reach out to CSA for clarification when there are differences in interpretation.

PREAMBLE

Feedback

2.26. Respondents sought clarification on the purpose of the preamble paragraphs included in each section, especially if the preamble paragraphs are to be included in the scope for the cybersecurity audit.

CSA's Response

2.27. The preamble paragraphs provide the domain context to the policy clauses in the following sections. The preamble is not in the cybersecurity audit.

3 COMPLIANCE REQUIREMENTS

AUDIT FINDING REMEDIATION PLAN

Feedback

3.1. Respondents sought clarification on fulfilling the requirements required by the audit finding remediation plan. For example, the mechanism for the CIIO to submit the remediation plan and the approval required before the CIIO carries out the remediation.

3.2. Respondents also sought clarification on the frequency of update for the audit finding remediation. For example, if the CIIO is required to provide an update upon completion of the remediation for each non-compliance or upon completion of all non-compliance audit finding, and whether a follow-up audit is required to be performed to verify the remediation status and thereafter a formal submission of follow-up audit report is required.

CSA's Response

3.3. All audit findings identified from the cybersecurity audit must be adequately and appropriately addressed in a timely manner. The CIIO is expected to provide an update upon completion of the actions taken to address each of the non-compliance until the completion of the audit finding remediation. Please refer to the latest Guidelines for Auditing Critical Information Infrastructure published on the CSA website.

3.4. Section 15(3) of the Cybersecurity Act, if any aspect of the audit appears to the Commissioner that was not carried out satisfactorily, the Commissioner may direct the CIIO to cause the auditor to carry out the aspect of the audit again.

Feedback

3.5. Respondents sought clarification on when the audit finding remediation plan is to be submitted to the Commissioner.

CSA's Response

3.6. The CIIO shall submit the audit finding remediation plans to the Commissioner within 30 days from the date that the CIIO receives the audit report from its auditors. The CIIO can proceed with the remediation plans unless CSA deems the remediation plans unsatisfactory. Please refer to the latest Guidelines for Auditing Critical Information Infrastructure published on the CSA website.

4 LEADERSHIP & OVERSIGHT

BOARD OF DIRECTORS & SENIOR MANAGEMENT'S OVERSIGHT AND MANAGEMENT OF CYBERSECURITY RISKS

Feedback

4.1. Respondents sought clarification on the knowledge and skills that the Board of Directors and Senior Management of the CIIO are expected to possess to manage the cybersecurity risks and ensure that effective controls are implemented to achieve cyber resiliency of the CII organisation.

4.2. Respondents sought clarification the ratio of members of the Board and senior management that requires cybersecurity knowledge.

CSA's Response

4.3. The CIIO is expected to have its Board of Directors ("BoD") to provide oversight of the cybersecurity risks and provide guidance its senior management on how to manage systemic risks, and the senior management to manage cybersecurity risks and ensure that controls are implemented.

4.4. The CIIO needs to ensure that both the BoD and senior management team include at least one member each that has the knowledge and awareness of cybersecurity matters to perform their functions effectively.

Feedback

4.5. Respondents enquired on the criteria and degree of knowledge and/or qualifications required to fulfil its compliance to the clause.

CSA's Response

4.6. The CIIO should develop its own criteria for BoD and senior management to have the necessary knowledge and awareness of cybersecurity matters to enable them to discharge their duties effectively. Some examples[1] may include whether the BoD and senior management have:

(a) obtained a certification, have qualification or expertise in managing cybersecurity risks;

(b) prior work experience in cybersecurity such as information security officer and security auditor; or

(c) knowledge, skills and other background in cybersecurity such as in areas of security policy and governance, security operations and risk management.

[1] Examples are adapted from U.S. Securities and Exchange Commission (SEC)

5 RISK MANAGEMENT

RISK MANAGEMENT FRAMEWORK – RISK CULTURE

Feedback

5.1. Respondents sought clarification on the criteria to measure organisation's risk culture and requested CSA to provide examples or references on how to fulfil compliance with the clause "*openly communicate risks, embrace learning from negative outcome, make informed decision when addressing risks in respective business context, carry out risk management effort that align with the defined risk appetite. These are critical success factor for risk management program"*.

CSA's Response

5.2. CSA has revised the clause for clarity. The CIIO is expected to establish an organisation's risk culture that includes enabling open communication of cybersecurity risks, embrace learning from positive and negative experiences, making informed decisions when addressing cybersecurity risks, and carrying out risk management efforts that commensurate with defined risk appetites. An organisation's risk culture is reflected in its behaviour toward negative outcomes: one with an effective risk culture will adopt a learning culture (i.e. learning from mistakes and treat the root cause) rather than a blame culture (i.e. assigning blame without identifying/treating the root cause of a problem).

RISK MANAGEMENT FRAMEWORK – THREAT MODELLING

Feedback

5.3. Respondents sought clarification on the steps required to perform threat modelling to identify threats to comply with clause *"Identification of cybersecurity threats with reference to the Guide to Cyber Threat Modelling or equivalent"* and clause *"Threats identified from threat modelling".*

CSA's Response

5.4. The CIIO can refer to "Guide to Conducting the Risk Assessment for CII" and "Guide to Cyber Threat Modelling" that CSA has published or their equivalent for guidance to identify threats through threat modelling. Broadly, threat modelling comprises the following steps:

(a) Step 1 – Scope Definition - which involves gathering information and demarcating perimeter boundary;

(b) Step 2 – System Decomposition - which involves identifying system components, drawing how data flows, and dividing out trust boundaries;

(c) Step 3 – Threat Identification - which involves identifying threat vectors and listing threat events; and

(d) Step 4 – Attack Modelling - which involves mapping sequence of attack, describing tactics, techniques and procedures.

RISK MANAGEMENT FRAMEWORK – ASSET IDENTIFICATION & PRIORITISATION

Feedback

5.5. Respondents enquired on the methodology and criteria for CIIO to reference when identifying and prioritising of CII assets.

CSA's Response

5.6. CSA has removed the need for prioritisation of CII assets. The CIIO should refer to the "Guide to Conducting the Risk Assessment for CII[2]" that CSA has published for guidance in the identification of assets. The asset inventory list should include all physical and logical assets of the CII.

RISK MANAGEMENT FRAMEWORK – RISK REGISTER

Feedback

5.7. Respondents commented that there are changes to the terminology used in the clause to document the risk register, as compared to the existing CCoP clause.

CSA's Response

5.8. Components and terms used in the risk register have been sharpened for clarity. CIIO may refer to Task B: Document Risk in the document Guide to Conducting Risk Assessment for CII for elaboration on populating the risk register.

[2] https://www.csa.gov.sg/-/media/Csa/Documents/Legislation_Supplementary_References/Guide-to-Conducting-Cybersecurity-Risk-Assessment-for-CII.pdf

RISK MANAGEMENT FRAMEWORK – PROCESS HAZARD ANALYSIS

Feedback

5.9. Respondents sought clarification on the definition, methodology, examples of cyber Process Hazard Analysis ("PHA") and the intent of having it incorporated into risk management process.

CSA's Response

5.10. The cyber PHA is a safety-oriented methodology for the assessment of the potential hazards associated with industrial processes that arise from cyber risks to the CIIO's OT systems. The outcome of the PHA is the identification of worst-case health, safety, and environment consequences to the OT environment, and any hazard scenarios arising from the cyber risks to the OT system. It is an approach based upon industry standards that includes ISA 62443-3-2, ISA TR84.00.09 and NIST SP 800-39.

5.11. The CIIO of an OT system needs to understand that the impact of a cybersecurity incident in an OT environment could not only affect the digital realm but also have health, safety, and environmental consequences. The intent of the clause is to ensure that the CIIO operating in an OT environment considers, incorporates into and addresses risk scenarios where the impact is on the health, safety, and environment aspects, in the cybersecurity risk assessment.

5.12. For example, an OT system can have multiple sensors monitoring the processes within the OT environment, which can be controlled from the Human Machine Interface ("HMI"). Compromise of these sensors by a cyber-attack such as a malware infection to the HMIs might result in health, safety, and environmental consequences as fires and other dangers remain undetected.

RISK MANAGEMENT FRAMEWORK – NON-DIGITAL ENGINEERING CONTROLS

Feedback

5.13. Respondents sought clarifications on the definition and examples of non-digital engineering controls that are to be incorporated into the risk management framework.

CSA's Response

5.14. Non-digital engineering controls refers to mitigating measures, of non-digital nature (e.g. analog), that help to reduce adverse impact in an OT environment. These controls are incorporated into OT systems to provide fault tolerance and prevent the OT from acting outside of acceptable parameters, reducing the impact that a digital incident on the OT might have.

5.15. The intent of the clause is to ensure that the CIIO operating in an OT environment incorporates non-digital engineering controls into the risk assessment.

5.16. For example, manual control mechanisms such as manual valve controls provide operators with the ability to manually control a pump without relying on the digital OT system. This ensures that the pump can still be controlled and functioning as intended even if the OT system has been compromised by a cybersecurity incident.

6 POLICIES, STANDARDS AND GUIDELINES

GAPS BETWEEN POLICIES AND PRACTICES

Feedback

6.1. Related to the clause *"The CIIO shall review the policies, standards, guidelines and procedures, against the current CII cyber operating environment and cybersecurity threat landscape, at least once every 12 months, from the completion of the last review",* respondents commented that organisations may face resource constraint due to many polices and standards put in place and high volume of CII related workload, thus requested CSA to reconsider to change the frequency of review from at least once every 12 months to at least once every 24 months.

CSA's Response

6.2. CSA recognised the technical and/or operational challenges to implement the revised heightened cybersecurity requirements. Unfortunately, the evolving cybersecurity threats have raised the need for more effective measures to further reduce cybersecurity risks to preserve the value of the business. As such, review of policies and standards against the cyber operating environment need to be performed on a timely basis or whenever there are changes to the cyber threat landscape to ensure its cybersecurity policies and standards continue to be relevant against the cybersecurity threats faced.

7 CYBERSECURITY DESIGN PRINCIPLES

DEFENCE-IN-DEPTH DESIGN PRINCIPLES

Feedback

7.1. Respondents sought clarification on CSA's expectation and guidance to demonstrate compliance to the defence-in-depth principle.

CSA's Response

7.2. Defence-in-depth is the use of a collection of multiple layers of security controls, including protective, detective and corrective controls, in the aspects of people, process and technology to protect the crown jewels of the organisation. This includes segregating the organisation network into different enclaves to break up a "flat" network to make the movement of attackers across the network more difficult. Each CIIO needs to assess cybersecurity risks of a CII and identify and implement relevant cybersecurity controls to reduce the cybersecurity risk levels to an acceptable level.

7.3. Specifically, the defence-in-depth principle is much like the "Castle approach" in medieval times. Before being able to conquer a castle, the intruder must beat the moat, drawbridge, towers manned by bowmen with arrows, etc. As such, each CIIO should ensure that the CII cyber operating environment has multiple proactive and defensive mechanisms spread across the people, process and technology domains to secure the CII. If one mechanism fails or has been compromised, another mechanism picks up the slack.

DEFENCE-BY-DIVERSITY DESIGN PRINCIPLES

Feedback

7.4. Respondents sought clarification on CSA's expectation and guidance to demonstrate compliance on the defence-by-diversity design principle. Some respondents asked about the type of diversity and extent of diversity that are required, or whether the diversity threshold can be determined by the CIIO.

CSA's Response

7.5. Defence-by-Diversity principle aims to reduce the number of potential attack vectors by having diversity throughout the CII, including diversity in technology, manufacturers and suppliers of assets, communication pathways, etc. For example, can use security systems from different vendors to reduce the chances of a common vulnerability, bug or configuration error that can be compromised by a single exploit. While this principle improves cybersecurity, employing multiple products could also increase the operating complexity and cost. The CIIO needs to balance these factors to determine the extent of diversity that is suitable for its use.

Feedback

7.6. Respondents suggested for CSA to add "*where possible*" to the clause to allow the CIIO the flexibility to comply with this principle.

CSA's Response

7.7. CSA qualified the clause with "to the extent possible". The CIIO could adopt a risk-based approach to prioritise the implementation of measures in its CII digital terrains with high-risk exposure.

SECURITY-BY-DESIGN PRINCIPLES

Feedback

7.8. Respondents sought clarification on whether if the Security-By-Design ("SBD") framework applies to only new CII systems, or the framework will also apply to the existing CII systems. Additionally, it is not possible to retrospectively apply new requirements on existing contracts that had been awarded to the vendors.

7.9. Respondents also sought clarification if the CIIO may adopt their own SBD framework or should be adopt CSA's SBD framework.

CSA's Response

7.10. CSA's SBD framework applies to new CII systems and to existing CII systems, throughout their lifecycles and especially when they are undergoing major enhancement and technology upgrades. For CII systems where it is not possible to retrospectively apply new requirements on existing contracts that had been awarded to the vendors, the CIIO should seek to factor this requirement into the contract as soon as possible and write to the Commissioner-in-charge-of-Cybersecurity to seek waiver for this clause.

7.11. The CIIO should adopt CSA's SBD framework. The CIIO may also adopt its SDB framework if the CIIO has reviewed and assessed that the framework is aligned with the CSA's SBD framework.

ZERO TRUST PRINCIPLES

Feedback

7.12. Respondents commented that zero trust principles are high-level tenets and sought clarification on CSA's expectation and guidance to demonstrate compliance on the zero trust design principles.

CSA's Response

7.13. The CIIO is not expected to undergo a network re-architecture in one go. Zero Trust Architecture works on the premise that trust is never granted implicitly but must be continuously evaluated. For example, each request to access data or service should be authenticated and authorised. If a request does not satisfy the access policy, the request is dropped; else, the request is accepted and a connection is established with this connection being continuously evaluated in real time. A change in security posture may result in the termination of the connection or re-authentication.

7.14. The approach of adopting zero trust principles can be different from CIIO to CIIO, depending on the risk profile of the organisation and nature of cybersecurity threats. The CIIO should take a risk-based approach to prioritise the implementation of measures to mitigate the cybersecurity risks.

Feedback

7.15. Respondents highlighted that it will not be feasible for the OT CIIO to apply zero trust principles on their existing systems due to system limitation and/or legacy issues.

CSA's Response

7.16. The clause for the zero-trust principle is qualified as "to the extent possible". CSA noted the respondents' feedback that there may be difficulties applying zero trust principles on existing systems due to system limitations or legacy issues. However, the CIIO should consider how it can utilise existing security infrastructure to implement security by design to achieve the zero trust principles without impending operations. The CIIO should assess the feasibility, conduct an assessment adopting a risk-based approach and determine the type of implementation that are best suited to apply the zero trust principles onto its CII systems.

CYBER STACK

Feedback

7.17. Respondents sought clarifications on CSA's expectations and guidance to demonstrate compliance on the review of cyber stack. The respondents also requested CSA to provide the cyber stack definition and the scope to review cyber stack.

7.18. Respondents enquired if Sectoral Threat Profile ("STP") is sufficient in performing the cyber stack review.

CSA's Response

7.19. CSA has reviewed and integrated the need to review cyber stack under the section "Risk Management". The CIIO should take a risk-based approach to review cyber stack. Through the conduct of a risk assessment, CIIO can review the adequacy of the existing security technologies to defend and respond to cybersecurity threats.

7.20. As part of the annual risk assessment, the CIIO can use the STP in the identification of cybersecurity threats that apply to the cyber stack.

Feedback

7.21. Some respondents enquired on what constitutes a material change in the CII cyber operating environment when reviewing the cyber stack.

CSA Response

7.22. The CIIO shall refer to the document "Supplementary Guidance on Notification of Material Change to CII" for guidance on what constitutes for material changes. If in doubt, the CIIO may approach Sector Officers for further clarifications.

CHANGE MANAGEMENT

Feedback

7.23. Respondents sought guidance on the scope of change management process.

CSA's Response

7.24. Effective change management process is essential for tracking and controlling changes made to the CII, including network security design, network connections, configuration settings, as well as program logic in both the CII hardware and software. Good change management process ensures that the current design and build state of these systems are validated and approved.

8 USE OF CLOUD

SCOPE OF CLOUD SECURITY REQUIREMENTS

Feedback

8.1. Respondents sought clarification whether the CII assets are required to be located in Singapore and if the cloud requirements apply to only new cloud systems or to existing CII systems already adopting cloud services.

CSA's Response

8.2. CSA has removed the clauses on the requirements of CII assets to be located in Singapore after taking into consideration the feedback from CIIOs and further consultation with the Cloud Service Providers. However, the CIIO shall remain responsible and accountable for maintaining oversight of the cybersecurity of the CII and for managing cybersecurity risks to the CII, even when the CII is wholly or partly implemented on cloud computing systems.

8.3. The scope of the cloud requirements will apply to all CII and will cover all cloud service models (e.g. IaaS, PaaS, and SaaS) and cloud deployment models (e.g. private, public, and hybrid). A CIIO considering use of the cloud services as part of its capability to deliver essential services will have to perform a detailed due diligence to understand the risks that comes along with using the cloud.

Feedback

8.4. Respondents also sought clarification whether the cloud service providers have to be a legally registered entity in Singapore.

8.5. Respondents have also enquired if the staff of the cloud service providers should be located in Singapore.

CSA's Response

8.6. CSA has removed the requirement for cloud service providers to be legally registered in Singapore. Instead, the policy requires the CIIO to ensure that the cloud service provider appoints a person within Singapore authorised to accept service of any notice or legal process relating to the provision of services to the CIIO on the service provider's behalf.

Feedback

8.7. Respondents enquired whether the use of cloud requirements are applicable to the cloud services used for OT CII.

CSA's Response

8.8. The cloud requirements apply to existing OT and IT CIIs that are already utilising cloud services and CIIs that will be moving to cloud.

Feedback

8.9. Respondents sought clarifications whether a recognised third-party cybersecurity audit report provided by the cloud service providers is sufficient for compliance with requirements in CCoP 2.0.

CSA's Response

8.10. The policy intent is for CIIO to implement the required cybersecurity controls to enhance the cybersecurity posture of its CII. The validation of the implementation of the controls shall be conducted through a cybersecurity audit regardless the CII is on-premises or in cloud. The approved auditor, when placing reliance on the third-party audit report, should review and ascertain that the third-party audit report covers the scope of the CCoP requirements.

MOVING CRITICIAL INFORMATION INFRASTRUCTURE TO THE CLOUD

Feedback

8.11. Respondents sought clarification on the consultation processes and mechanisms required to submit to Commissioner and guidance of the risk assessment framework when planning to adopt cloud service as well as the frequency to conduct the risk assessment.

8.12. Respondents sought clarifications whether an approval from the Commissioner is required:

(a) when a CIIO plans to move CII to the cloud; and

(b) for the remediation plan to carry out rectification works to rectify aspects of the cybersecurity risk assessments that were assessed by the Commissioner.

CSA's Response

8.13. The CIIO planning to adopt cloud services shall inform Commissioner. This must be done before any preparation steps are taken to adopt cloud services for its CIIs. Thereafter, CSA will provide guidance on the scope of the risk assessment and/or due diligence exercise that needs to be performed by the CIIO.

8.14. While the risk assessment is a one-time exercise as part of the CIIO's due diligence when planning to adopt cloud services for its CIIs, the risk assessment should be re-performed if the CII cyber operating environment on the cloud changes.

8.15. The CIIO is not required to seek approval from the Commissioner when planning to move CII to the cloud. The CIIO is expected to inform the Commissioner of any plans before moving CII to the cloud and to submit a completed cybersecurity risk assessment to the Commissioner for review within 30 days of completion. Where it appears to the Commissioner that any part of the cybersecurity risk assessment was not carried out satisfactorily, the CIIO has to complete rectification works to the Commissioner's satisfaction at the CIIO's own cost and within the timeframe(s) specified by the Commissioner.

9 OUTSOURCING AND VENDOR MANAGEMENT

OVERSIGHT OVER VENDOR MANAGED CII ACTIVITIES

Feedback

9.1. Respondents sought guidance on the implementation to provide oversight on vendor managed CII activities, such as whether CCTV monitoring and logging are sufficient to comply with the CCoP requirements.

CSA's Response

9.2. The CIIO should consider all types of controls that allow them to have an oversight over vendor-managed CII activities. These controls include preventive, detective, structural, procedural and technical measures. The intent is to minimise the risk that the vendors may introduce into the CII environment. For example, vendors may connect their maintenance devices into the CII network for diagnostics and this may inadvertently introduce security vulnerabilities into the CII network. The CIIO should assess the risk related to vendor managed CII activities and put in place the necessary controls to meet the policy intent.

SUPPLY CHAIN RISK ASSESSMENT

Feedback

9.3. Respondents sought clarification on the need to conduct a supply chain risk assessment in addition to the annual cybersecurity risk assessment.

CSA's Response

9.4. CSA has revised the clause for clarity. CSA expects the CIIO to include cybersecurity risk scenarios related to supply chain as part of the annual cybersecurity risk assessment requirements under the Cybersecurity Act. The policy intent is to ensure that the CIIO understand and manage the supply chain risks that the organisation is exposed to.

CYBERSECURITY REQUIREMENTS FOR VENDORS

Feedback

9.5. Respondents sought clarification on the following:

(a) if the obligations of a vendor to protect the CII against cybersecurity threats and to report cybersecurity incidents apply to existing contractual terms with the vendor;

(b) if the obligations of a vendor to protect the CII against cybersecurity threats and to report cybersecurity incidents could be complied through means of tender specifications;

(c) the scope to conducting audit on vendors; and

(d) if the rights to commission an audit on a vendor are applicable to existing contractual terms.

CSA's Response

9.6. The CIIO is accountable for the CII's cybersecurity posture, even if the CIIO has outsourced any aspect of its activities to a third-party vendor. Hence, this is applicable for all services rendered.

9.7. The policy intent is to ensure that the CIIO maintains oversight over the vendor managed CII activities and implement appropriate cybersecurity controls for mitigating the cybersecurity risk exposure originating from the vendor.

9.8. The policy intent of having rights to commission an audit of a vendor's cybersecurity posture is to ensure that the CIIO is able to ensure that the vendor has implemented the required cybersecurity controls to enhance its cybersecurity posture. This could include an audit on the vendor's cybersecurity posture or obtaining a recognised cybersecurity audit report prepared by a third party.

10 ASSET MANAGEMENT

ASSET INVENTORY REQUIREMENTS

Feedback

10.1. Respondents sought clarification on the following:

(a) whether the asset inventory covers only assets within the CII boundary, or it also covers assets that have connections with the CII; and

(b) whether the CII Information Record form reflects the asset inventory requirements.

CSA's Response

10.2. The CIIO shall ensure that its asset inventory includes all CII assets, including any other asset under the CIIO's control that is directly connected or communicates with the CII.

10.3. All asset inventory requirements can be found in CII Information Record Form[3] that was published on CSA's website.

[3] https://www.csa.gov.sg/-/media/Csa/Documents/Legislation_Forms/CII-Information-Record-Form.xlsx

Feedback

10.4. Respondents sought clarifications if the asset inventory requirements are required for CII in cloud.

CSA's Response

10.5. Yes, the asset inventory requirements are applicable to CII, whether deployed in whole or in part, in cloud. The scope of the requirements applies to all cloud service models and cloud deployment models. The CIIO shall furnish information of the CII to the Commissioner as required under section 10(1) of the Cybersecurity Act.

10.6. The intent is to ensure that the CIIO has visibility of all CII assets within a CII, including their functions, dependencies and connectivities to one another and external systems and networks. This information allows the CIIO to defend the network through conducting risk assessments on CII assets and their dependencies and then addressing these risks.

11 PROTECTION REQUIREMENTS

ACCESS CONTROL MANAGEMENT

Feedback

11.1. Respondents sought clarification on the following:

(a) whether the scope of user access management process and the mechanisms to perform periodic reviews include external users (e.g. vendors and contractors);

(b) the frequency of regular/periodic review for user access;

(c) the definition and scope of the phrase "*anomaly in the user behavioural patterns*";

(d) it might be operationally challenging to restrict the installation of software to only administrator accounts;

(e) the definition of "inactive account"; and

(f) the criteria of "sensitivity" in terms of activities performed by shared user accounts.

CSA's Response

11.2. The CIIO is expected to perform periodic reviews for all accounts that are used in the CII environment. This is to ensure that accounts used in the CII environment are valid and privileges assigned are granted at the minimum required to perform the assigned duties and functions.

11.3. The frequency of the review is at least once every 12 months to evaluate the validity of accounts and to ensure that privileges assigned to each account are up-to-date.

11.4. The CIIO is expected to monitor the behavioural patterns of user accounts within the CII environment and to trigger an alert if a CIIO detects suspicious behaviour patterns or behaviour patterns that deviate from the expected baseline.

11.5. The clause has been revised to ensuring that only accounts authorised to install software are given the rights to reduce the risk of unauthorised software installations.

11.6. An inactive account refers to any account that is no longer required. For example, accounts of employees who had left the organisation.

11.7. CSA has revised the clause for clarity. The frequency of review shall commensurate with the frequency of activities performed by the shared user account.

Feedback

11.8. Respondents commented that it may not be possible to delete or disable inactive accounts due to product and system limitations.

CSA's Response

11.9. While there are inherent system constraints that disallow the deletion or disabling of inactive accounts, a CIIO can consider implementing other compensating measures such as monitoring access and activities of inactive accounts. The intent of the clause is to mitigate the risks of threat actors accessing CII network using inactive accounts.

PRIVILEGED ACCESS MANAGEMENT

Feedback

11.10. Respondents sought clarification on the following:

(a) whether the requirement to maintain an inventory of privileged accounts, permissions, and privileges applies only to CII or to the entire CII organisation;

(b) the scope and requirements to log all privileged access and activities to identify anomalous activities; and

(c) the definition of emergency accounts.

CSA's Response

11.11. The CIIO is expected to maintain an inventory of all privileged accounts with details of the accounts' permission and privileges assigned to the CII assets. While the clause is only applicable to the CII, the CIIO should consider extending the inventory exercise to the entire CII organisation because privileged accounts, which are prime targets for malicious exploitation, are also found beyond the CII boundary.

11.12. The intent of the clause is to facilitate early detection of any unauthorised access and malicious activities performed by the privileged accounts. The CIIO should log privileged account related activities such as login attempts, configuration changes etc.

11.13. CSA has removed the clause "*The CIIO shall ensure that approval is sought when use of emergency account is required"*. The use of emergency accounts should have already been authorised when the accounts were first created.

NETWORK SEGMENTATION AND SECURITY

Feedback

11.14. Respondents sought clarification on the following:

(a) whether the clause on segmenting the CII network architecture into different network zones based on functionality and the security level applies to existing CII systems or new CII systems;

(b) whether the requirement to limit the direction of data flow, if only one-way data flow is required, can be fulfilled by the implementation of a common firewall; and

(c) whether the requirement to implement network security devices between the different network zones to secure the network communication is applicable to cloud-based setup with no access to manage the network level.

CSA's Response

11.15. The clause on segmenting the CII network architecture into different network zones applies to all CII systems, including existing CII systems and new CII systems.

11.16. The intent of the clause is to mitigate the risks of malicious and unauthorised network traffic into the CII environment. The CIIO is required to perform its own assessment if the common firewall can fulfil the policy intent to be used in its CII cyber operating environment. Some examples include firewall, data diode or other similar technologies to restrict the data flow.

11.17. The requirement to implement network security devices between the different network zones applies to all networks within the CII boundary.

REMOTE ACCESS MANAGEMENT

Feedback

11.18. Respondents sought clarification on the following:

(a) whether the clauses for remote connection to implement cybersecurity measures applies to user connection and/or system-to-system connection;

(b) what would qualify as an authorised source of remote connections to the CII;

(c) the intent for remote connection to CII through secured intermediary mechanism;

(d) examples of approach and types of files to be scanned for malware before uploading to the CII via remote connection; and

(e) examples of what to be included in the logging of all remote access and activities to CII for the monitoring and detection of cybersecurity events.

CSA's Response

11.19. The clauses to implement cybersecurity measures for remote connections applies to all remote connections to the CII, including both user connection and system-to-system connection.

11.20. CSA has revised the clause for clarity. The intent of the clause is to ensure that only legitimate/approved and known sources are allowed to have remote connection to the CII.

11.21. The intent of enabling remote connection to CII through secured intermediary mechanism is to mitigate the risks of remote connection acting as a direct conduit for cyber threat actors to access the CII.

11.22. The CIIO shall scan files before uploading files to the CII to ensure that malware is not introduced to the CII whenever a file is uploaded to the CII. The CIIO may take reference from industry standards or best practices such as NIST, ISO etc.

11.23. The intent to log and monitor the remote connection is to detect any unauthorised access and malicious activities to the CII. The CIIO should retain relevant security logs to meet the policy intent. Examples of logs include login attempts, VPN connections, etc.

WIRELESS COMMUNICATION

Feedback

11.24. Respondents sought clarification on the following:

(a) if wireless communication refers to wireless LAN within the CII or it includes other communication protocols such as Bluetooth, mobile 4G/5G etc; and

(b) whether the scope covers employee connecting to the CII or the corporate network.

CSA's Response

11.25. Wireless communication refers to use of wireless LAN within the CII. The scope includes employees connecting to CII through wireless LAN. CIIO's corporate network is not covered within the scope of section 5.8. However, CSA has included wireless communication related clauses in Annex A of the CCoP 2.0 document as guidance for the CIIO to consider and implement beyond the CII boundary.

SYSTEM HARDENING AND SECURITY CONFIGURATION

Feedback

11.26. Respondents sought clarification on the following:

(a) the approach to apply revised security baseline configuration standards while maintaining availability of existing CII; and

(b) the minimum password length to constitute as a passphrase to avoid ambiguity.

CSA's Response

11.27. The CII cyber operating environment and cybersecurity threat landscape of each CII environment varies. As such, the CIIO should perform its own assessment and apply the configuration changes to the existing CII assets in accordance with its established change/configuration management policies and procedures.

11.28. The CIIO may take reference from industry standards or best practices such as NIST to determine the appropriate password length.

Feedback

11.29. Respondents commented on the following:

(a) some CII assets use proprietary operating systems which does not have security baseline configuration standards for reference; and

(b) it is operationally risky to always use the latest version of anti-malware software without proper testing.

CSA's Response

11.30. Establishing baseline security configuration standard allows the CIIO to ensure that CII assets are configured securely to reduce the attack surface. This will also ensure that the security configurations on CII assets are consistent. The CIIO could take reference from reputable sources (e.g. Center for Internet Security (CIS) Benchmarks) when establishing baseline security configuration standards that are tailored to its CII assets. If there is no readily available source (i.e., proprietary systems) to reference from, the CIIO should seek guidance from the vendor for recommended security baselines and determine the relevant configurations to be included in the security baseline configuration standards.

11.31. As per any proper change management process, the CIIO should always test the latest version of anti-malware software in an environment that is similar to the CII production environment to ensure the software does not cause any unintended consequences (e.g. disruption to the Essential Service) when it is installed in the CII production environment.

PATCH MANAGEMENT

Feedback

11.32. Respondents sought clarification on the following:

(a) the CIIO may not have a test environment that is similar to the production environment to test all security patches; and

(b) the approach to verify legitimacy of the patches and if the verification of patches applies to open-source products.

CSA's Response

11.33. Security patches should always be tested to ensure that the patches do not cause any unintended consequences when they are installed. If a proper testing environment is not available, the CIIO is expected to implement other compensating measures. The CIIO may consider having a backup system to fallback to in the event that a security patch causes a service disruption or putting in place monitoring mechanisms when patching is not possible.

11.34. The intent is to minimise the likelihood of threat actors embedding malware onto the patch. The verification of patches applies to all patches to CII assets, including open-source products. CSA has revised the clause to omit the verification of the legitimacy of the patches. However, the CIIO is required to verify the integrity of the patches. An example to verify the integrity of the patch is by checking its digital signature.

PORTABLE COMPUTERS AND REMOVABLE STORAGE MEDIA

Feedback

11.35. Respondents commented that it is impractical to enforce CIIO's system hardening standards on vendor's laptops or portable computing devices, especially when the laptops contain specialised tools to be used for troubleshooting. These tools are intellectual property, and the vendor would not allow them to be installed locally on CIIO-owned laptops.

CSA's Response

11.36. The CIIO should ensure that all portable computers connecting to the CII are secured. This is to minimise the likelihood of it being used a medium for threat actors to deliver malware to the CII systems or networks. The CIIO should perform their due diligence and risk assessment to decide on the mitigating measures to put in place to meet the policy intent.

APPLICATION SECURITY

Feedback

11.37. Respondents sought clarification on the following:

(a) whether the requirements to reference the latest application security guidelines when designing, developing, and testing application applies to only web-based application;

(b) whether the implementation of Web Application Firewall (WAF) applies only to internet-facing and public-facing systems;

(c) the approving authority to approve applications used for the purpose of operation and the cybersecurity of the CII; and

(d) the types of application access and activities logs to be maintained and monitored.

CSA's Response

11.38. Yes, the requirement to reference the latest application security guidelines when designing, developing, and testing application applies only to web-based CII applications.

11.39. Yes, the Web Application Firewall (WAF) shall be implemented on internet-facing web-based CII systems.

11.40. The CIIO should follow its organisation policies and processes to approve only applications that are used for the purpose of operation and the cybersecurity of the CII.

11.41. The CIIO should log and monitor all application access and activities to detect any unauthorised access or malicious activities to the application. Following the feedback, CSA has revised the clause to provide clarity.

DATABASE SECURITY

Feedback

11.42. Respondents sought clarification whether the same individual can be database administrator and system administrator.

CSA's Response

11.43. Segregation of duties is a key concept of internal controls to ensure checks and balances for preventing fraud and errors. An individual should not be both a database administrator and system administrator as excessive access could increase the risk of abuse if the access is misused or compromised.

VULNERABILITY ASSESSMENT

Feedback

11.44. Respondents sought clarification on the following:

(a) whether the scope of the vulnerability assessment is applicable to the CII assets only;

(b) if the vulnerability assessment should include scanning against CVE signatures and security standards; and

(c) examples of major system changes.

CSA's Response

11.45. The conduct of vulnerability assessment applies to all CII assets.

11.46. The CIIO should identify security and control weaknesses in the CII assets. The vulnerability assessment should include scanning against CVE signatures and security baseline configuration standards.

11.47. CSA has included examples of major system changes in the CCoP 2.0. The CIIO may also take reference from CSA's Supplementary Guidance on Notification of Material Change to CII document for examples of major system changes.

PENETRATION TESTING

Feedback

11.48. Respondents highlighted the challenges of conducting penetration testing in Operational Technology (OT) environment due to the potential implications on system availability and safety of the operations. The respondents also requested for a set of procedures to conduct penetration testing for OT systems and recommended/registered list of vendors to perform the penetration testing in Singapore.

11.49. Respondents sought clarification on the rationale to supervise penetration testing conducted by third-party penetration testing service providers.

CSA's Response

11.50. Penetration testing allows the CIIO to identify weaknesses and vulnerabilities in the CII. If there are potential safety and reliability concerns, the CIIO is expected to explore other compensating measures to meet the intent. These includes having monitoring mechanisms for early detection, having recovery measures in placed or ensuring CIIs are patched promptly, etc. When selecting a suitable vendor for penetration testing, the CIIO should consider the vendors' experience in OT penetration testing.

11.51. The intent of having penetration testing to be conducted under the supervision of the CIIO is to ensure that the penetration testing is conducted in accordance with the rules of engagement defined.

RED OR PURPLE TEAMING/ADVERSARIAL ATTACK SIMULATION

Feedback

11.52. Respondents sought clarification on whether:

(a) red teaming can be in the form of a table-top exercise;

(b) it is acceptable for CIIO's with multiple OT CII to conduct red teaming for just one CII every 24 months; and

(c) red teaming is applicable to CII that is always shutdown unless during maintenance and scheduled activities.

CSA's Response

11.53. The red team exercise should be conducted through attack simulations to assess the organisation's resilience against such adversarial attack TTPs. The intent is to provide a realistic picture of the organisation's capability to prevent, detect and respond to real adversaries by simulating the TTPs of real-world attackers targeting people, processes and products technology underpinning the critical functions in the organisation. A CIIO can conduct purple team exercises if they are not ready for red team exercises. CSA has revised the clause to include purple teaming. The CIIO should progressively move to red teaming when they are more prepared.

11.54. The CIIO is expected to assess and determine the implementation approach to conduct red teaming for its CII to meet the policy intent.

11.55. The requirement to conduct red team or purple team exercise applies to all CII, regardless of the system status (i.e., active or inactive).

CRYPTOGRAPHIC KEY MANAGEMENT

Feedback

11.56. Respondents sought clarification on whether:

(a) protecting cryptographic key against unauthorised access, modifications and deletions is only applicable for internet-facing web applications; and

(b) protecting cryptographic key is required when there is an air gap in the system.

CSA's Response

11.57. The CIIO is required to protect cryptographic key against unauthorised access for all CII that uses cryptographic keys, including air gap system.

DOMAIN NAME SYSTEM SECURITY EXTENSION (DNSSEC)

Feedback

11.58. Respondents sought clarification on the following:

(a) if DNSSEC only applies to internet-facing CII; and

(b) if ensuring DNSSEC-signed on the domain names is applicable for CII that does not use DNS and DNS services.

CSA's Response

11.59. The DNSSEC requirements have been shifted to Domain-Specific section in CCoP 2.0 and the DNSSEC requirements are only applicable to CII with internet-facing DNS servers within its CII boundary.

12 DETECTION REQUIREMENTS

LOGGING REQUIREMENTS

Feedback

12.1. Respondents sought clarification on the following:

(a) if the CIIO is required to have high availability for its logs retention;

(b) definition of regulatory requirements to be taken in consideration with regard to log retention period; and

(c) type of logs to retain.

12.2. Respondents enquired on the retention of the logs and the processes and mechanisms to send the logs to Commissioner.

CSA's Response

12.3. The intent is to ensure that the CIIO establishes a policy for log retention to facilitate investigation. CSA does not prescribe if high availability is needed for the log retention servers. CSA expects the CIIO to assess and determine the appropriate mechanisms required to comply with the requirement.

12.4. CSA noted the respondents' feedback to request for more guidance with regard to the definition of regulatory requirements to be taken into consideration to retain the logs and the type of logs to retain. CSA has revised the logging requirements. For example, the retention period of the logs to be a minimum period of 12 months (cl 6.1.4.C) and the type of logs are specified in each domain section in CCoP 2.0 (e.g. cl 6.1.1).

Feedback

12.5. Respondents requested for the CIIO to allow logs to be filtered and desensitised before sharing with the Commissioner.

CSA's Response

12.6. The intent is to make the raw logs available for the Commissioner to do sense making to identify systemic cyber risks across the CII sectors and elaborated cyber campaigns that could impact multiple sectors. Therefore, the raw logs should not undergo any further processing.

MONITORING AND DETECTION

Feedback

12.7. Respondents sought clarification on the following:

(a) if each CII can have its own mechanisms and processes to detect, collate and analyse cybersecurity events;

(b) if scanning of indicators of compromise ("IOCs") provided by CSA and/or Sector Leads are sufficient to meet the requirement of the clause; and

(c) if collating of all cybersecurity events in a centralised location refers to storing of these events in a centralised location.

CSA's Response

12.8. CSA expects the CIIO to assess and determine the appropriate mechanisms required to comply with this requirement.

12.9. The CIIO is required to scan the IOCs provided by CSA and Sector Leads. The CIIO is encouraged to tap onto other threat intelligent sources to broaden their detection effectiveness.

12.10. CSA has revised the clause for clarity. While CSA has removed the need to store cybersecurity events in a centralised location, the intent remains that CIIOs are to collect and store records of cybersecurity events, to analyse and correlate these cybersecurity events to determine whether there is or has been any cybersecurity incident.

THREAT HUNTING

Feedback

12.11. Respondents sought clarification on the following:

(a) whether threat hunting is similar to the Cyber Threat Modelling that CSA has advocated earlier;

(b) is there a need to conduct threat hunting on all CIIs;

(c) is the cybersecurity risk assessment mentioned in the threat hunting section referring to the annual risk assessment mandated under the Cybersecurity Act; and

(d) can CSA provide guidance on threat hunting.

CSA's Response

12.12. Threat modelling is a structured process for identifying threat events while threat hunting is the proactive effort to search for signs of malicious activity that have evaded security defences within the CII.

12.13. The CIIO is required to conduct threat hunting on all CIIs.

12.14. The cybersecurity risk assessment mentioned in the threat hunting section refers to the annual risk assessment mandated under the Cybersecurity Act.

12.15. Examples of the components of the threat hunting include having data to baseline normal traffic to find outliners, develop hypothesis based on tools and framework, and investigate and analyse potential threats to discover any new malicious patterns in the data and uncover threat actor's TTPs.

Feedback

12.16. Respondents also highlighted that the clause mandates threat hunting to be conducted at least once every 24 months, but the CIIO is required to conduct cybersecurity risk assessment once every 12 months. Hence, the CIIO is unable to comply with the requirement to conduct risk assessment based on threats identified from threat hunting since the frequency for conducting threat hunting and risk assessment are not aligned.

CSA's Response

12.17. CSA acknowledges that the threat hunting frequency is not aligned with the risk assessment cycle. Threat hunting is to address cybersecurity threats that could be lurking undetected on the network, whereas risk assessment is to address potential cybersecurity threats. These two are not meant to be sequential because they are designed for different purposes.

CYBER THREAT INTELLIENCE AND INFORMATION SHARING

Feedback

12.18. Respondents sought clarification on the following:

(a) the requirement "to conduct threat intelligence" and if the CIIO needs to have threat intelligence capability to conduct threat intelligence; and

(b) if the controls to mitigate the cybersecurity threats identified from the threat intelligence refer to the existing controls in place and if compensating controls can be used if the relevant controls are not implementable.

CSA's Response

12.19. The CIIO is required to establish mechanisms and processes to collect threat intelligence for its CII. Threat Intelligence includes cybersecurity threat activities and vulnerabilities.

12.20. Threat intelligence provides contextual information that enable an organisation to take proactive actions to prevent or mitigate cyber-attacks. It involves obtaining an understanding of trending threat landscapes, threat actors and their Tactics, Techniques and Procedures (TTP) to translate them into actionable contextualised information for early warning and detection. If a CIIO does not have in-house capabilities to conduct threat intelligence, it can consider procuring threat intelligence from vendors or tap into community sources such as Information Sharing and Analysis Centers (ISACs) or open sources such as SANS Internet Storm Center and DHS CISA Automated Indicator Sharing, over and above those provided by CSA and Sector Leads. Having more threat intelligence sources could also result in having a better resolution of the threat actor's motivation and TTPs.

12.21. The intent is to ensure that the CIIO implements adequate controls to mitigate cybersecurity threats and vulnerabilities identified from threat intelligence. The CIIO is expected to assess and determine the type of controls required to mitigate the identified threats and vulnerabilities.

Feedback

12.22. Respondents highlighted that the procedures and mechanisms for sharing information on cybersecurity threats with the Commissioner need to be agreed bi-laterally and suggested for a framework to be established for the bi-lateral sharing of information with the Commissioner.

CSA's Response

12.23. CSA will work with sector leads to provide guidance for the CIIO to share threat intelligence with the Commissioner.

13 RESPONSE AND RECOVERY REQUIREMENTS

CYBER INCIDENT MANAGEMENT

Feedback

13.1. Respondents sought clarification on the following:

(a) the types of cybersecurity incidents that would trigger stakeholders such as external media;

(b) if the requirement for communication and coordination structure for members of the Cybersecurity Incident Response Team and senior management in the Incident Management section is a duplicate requirement in the Crisis Communication Plan;

(c) CSA's expectation on the timeline to complete the post-incident review to identify and implement corrective measures to prevent a recurrence;

(d) the rational in updating the incident response plan's review frequency to once every 12 months in CCoP 2.0, and in what circumstances will the CIIO needs to review the incident response plan; and

(e) if its organisation is allowed to define the triage framework based on operational and business needs.

CSA's Response

13.2. The CIIO should assess and determine the type of cybersecurity incidents that will have a significant impact on public perception or will trigger the attention of external media. The CIIO should work with their communication teams to establish a communication plan to provide consistent and coordinated view of the cybersecurity incident to the external media.

13.3. The intent of the two communication and coordinated structure are different. Having a communication and coordination structure in the incident response plan is to ensure that cybersecurity incidents can be escalated in a timely manner while having the communication and coordination structure in the crisis communication plan is to ensure that responses, during crises, are coordinated and consistent.

13.4. The post-incident review should be completed together with the implementation of corrective controls in a timely manner to prevent recurrence of similar cybersecurity incidents. While this is taking place, the CIIO should put in place compensating controls to address the risks that were exploited.

13.5. The evolving cybersecurity threats have raised the need for increased frequency to ensure the incident response plan remains updated and relevant. Therefore, CSA has revised the review period to 12 months.

13.6. CIIO is allowed to assess and determine the appropriate actions and scope required to establish a triage framework to fit the organisational needs. The triage framework should include:

(a) analysing all cybersecurity events;

(b) correlating between cybersecurity events;

(c) determining whether there is or has been any cybersecurity incident; and

(d) triggering applicable incident reporting, response and recovery plans if there is or has been any cybersecurity incident.

Feedback

13.7. Respondents requested guidance on the following:

(a) the definition of “trained” and if the Cybersecurity Incident Response Team (CIRT) needs to undergo training courses and be certified; and

(b) the type of change that is required to trigger the review of the incident response plan.

CSA’s Response

13.8. The purpose of a trained CIRT is to respond timely to a cybersecurity incident to try to stop the attack in its track, minimise impact and restore operations quickly. The CIIO should have adequate CIRT training programs in place to ensure that personnel have the requisite skills and competence which commensurate with their respective roles and responsibilities. The CIIO can consider technical trainings from institutions such as SANS, Group-IB etc.

13.9. Changes to the incident response plan will require a review of the plan. For example, changes to the Cyber Incident Response team (CIRT) structure.

Feedback

13.10. Respondents commented on the following:

(a) there may be instances where it may not be operationally feasible to collect and preserve digital forensic evidence and recommend an amendment to the clause to add "where possible"; and

(b) if the monitoring and detection is done by external Managed Security Service Provider (MSSP), the triage framework should be from MSSP instead of CIIO.

CSA's Response

13.11. The digital forensic evidence should be collected and preserved to support investigations and for legal admissibility purposes. As such, the CIIO is expected to assess and determine appropriate procedures that fit their operational needs to collect and preserve forensic evidence, as well as ensuring chain of custody requirements and legal requirements are met.

13.12. CSA expects the CIIO to be accountable for the triage framework. While the CIIO may delegate the monitoring and detection function to a third-party service provider, the CIIO is still accountable and responsible for the triage framework.

CRISIS COMMUNICATION

Feedback

13.13. Respondents sought clarification on the following:

(a) the scope of the crisis communication training;

(b) the intent of including alternate mode of communication in the Crisis Communication Plan and the alternate mode of communication required in the event the primary mode of communication is compromised;

(c) if the mode of communication refers to internal or external communication channel; and

(d) if the crisis communication plan applies to all cybersecurity incidents of all severity.

CSA's Response

13.14. Examples of the scope of the crisis communication training could include, but not limited to, success factors of an effective spokesperson, effective pitches to the press and stakeholders, managing media conferences or panel discussions. The CIIO is to assess and determine the appropriate training programs to ensure that personnel have the requisite skills and competencies to execute the crisis communication plan ensuring coordinated and consistent responses during a crisis to its CII organisation.

13.15. Alternate mode of communication refers to a separate communication channel that the CIIO can use in the event their primary mode of communication is not available. The CIIO is expected to assess and determine the appropriate methods to keep the communication channels open in the event the primary mode of communication is compromised.

13.16. The CIIO should take into consideration all relevant stakeholders including both internal and external parties.

13.17. The goal of the crisis communication plan is to ensure communications are coordinated and consistent to all stakeholders during a crisis. The CIIO should work with their communication teams to assess and determine the type of cybersecurity incidents that have significant impact and require the activation of the crisis communication plan to respond to the crisis. Some examples include cybersecurity incidents with reputation risks and cybersecurity incidents that lead to loss of life.

CYBERSECURITY EXERCISE

Feedback

13.18. Respondents sought clarification on the following:

(a) if the CIIO is to conduct the Business Continuity Plan ("BCP"), Disaster Recovery Plan ("DRP"), incident management plan and crisis communication plan in the same cyber exercise;

(b) the CIIO is not required to participate in any national/sectoral exercise moving forward if the expectation is for CIIO to conduct annual exercise; and

(c) if all CII under the CIIO is required to be exercised in the annual cybersecurity exercise.

CSA's Response

13.19. The intent of the clause is to ensure that the CIIO exercises the BCP, DRP and incident management and crisis communication plan requirements. The CIIO is to assess and determine if more than one cybersecurity exercise is needed.

13.20. The intent mandates the CIIO to conduct annual cybersecurity exercise(s) at its organisation level. The requirement for the CIIO to participate in a cybersecurity exercise if directed in writing to do so by the Commissioner is mandated under the Cybersecurity Act.

13.21. The CIIO is expected to exercise all CII in the annual cybersecurity exercise(s). The continuous cycle of assessment, validation and improvement of the plans through a regular cybersecurity exercise regime for all its CII will improve the operational readiness of the organisation. This will enable the organisation to respond swiftly and effectively to a cybersecurity incident.

BACK UP AND RESTORATION

Feedback

13.22. Respondents sought clarification on the following:

(a) if the cause of system disruptions or data corruption mentioned in the backup and restoration plan is referring to cybersecurity incident;

(b) the frequency that the CIIO needs to test of the restoration of the backups; and

(c) if the backups can be stored in the same premises.

CSA's Response

13.23. The backup and restoration plan needs to take into considerations all events that can potentially affect the CII's ability to deliver essential services and is not limited to only cybersecurity incidents.

13.24. CSA has revised the clause for clarity. The CIIO is expected to perform the restoration test at a pre-defined interval that commensurates with the cybersecurity risk profile of the CII.

13.25. The CIIO should conduct a risk assessment and determine the appropriate location to store the backups and ensure the backups are protected from unauthorised access, modification and deletion.

Feedback

13.26. Respondents commented that it will be operationally infeasible to test the backup restoration if there is no testing environment available.

CSA's Response

13.27. The intent is to ensure that the backups can be restored when required. If testing of backup restoration is not implementable due to operational or business considerations, the CIIO should write to the Commissioner-in-charge-of-Cybersecurity to seek waiver for this clause and use compensating controls that mitigate relevant risks accordingly.

BUSINESS CONTINUITY AND DISASTER RECOVERY

Feedback

13.28. Respondents sought clarification if the CIIO is still required to conduct BCP and DRP exercises as the requirement to conduct BCP and DRP exercises has been omitted from the BCP and DRP section.

CSA's Response

13.29. The CIIO is still required to conduct BCP and DRP exercises and the requirement is now covered under the Cybersecurity Exercise section.

ACTIVE DIRECTORY/DOMAIN CONTROLLER

Feedback

13.30. Respondents sought clarification on the following:

(a) whether there is a need to establish the recovery procedures for the compromise of the domain controller's Kerberos Ticket Granting Ticket if there is no domain controller in the CII environment;

(b) the intent of including specific recovery procedure scenario for the domain controller; and

(c) if the exercise of the recovery procedures for the compromise of the Kerberos Ticket Granting Ticket as part of the DR exercise needs to be on actual recovery procedures.

CSA's Response

13.31. The CIIO is expected to establish the recovery procedures if the domain controller is used by the CII assets, regardless of whether the domain controller is implemented inside or outside the CII environment. This is to ensure that the CIIO is well prepared with the procedures to reset the Kerberos Ticket Granting Ticket account in the event of a cybersecurity incident.

13.32. The intent to include specific recovery procedure for Kerberos Ticket Granting Ticket account is to ensure that the CIIO is prepared with the procedures to reset the Kerberos Ticket Granting Ticket account in the event of a cybersecurity incident.

13.33. With the establishment of the recovery procedures for Kerberos Ticket Granting Ticket account, the CIIO is expected to exercise the procedures in cybersecurity exercise.

14 CYBERSECURITY TRAINING & AWARENESS

TRAINING BASED ON ROLES IN CII ORGANISATION

Feedback

14.1. Respondents enquired on the cybersecurity skillsets and training that the personnel working in the CII organisation are required to attend.

CSA's Response

14.2. CSA expects the CIIO to have adequate cybersecurity training programs in place to ensure that personnel have the requisite skills and competencies which commensurate with their respective roles and responsibilities. Some examples of commercial training sources include, but not limited to, SANS, ISACA and ISC[2.]

CERTIFICATIONS FOR CYBERSECURITY RISK ASSESSMENT AND AUDIT

Feedback

14.3. Respondents sought clarification on the following:

(a) the certifications that are required for the personnel engaged to conduct cybersecurity risk assessment and cybersecurity audit; and

(b) the composition of the cybersecurity audit team that required to be certified to perform the audit on CII.

CSA's Response

14.4. Industry-recognised certifications include CISA, CRISC or equivalent certifications. The CIIO is expected to identify the industry-recognised certifications as appropriate. Professional certifications provide a means for the CIIO to assess the competency of the personnel engaged to conduct cybersecurity risk assessment and cybersecurity audit of the CII.

14.5. CSA has revised the clause to indicate that the personnel overseeing the conduct of the cybersecurity audit needs to be certified. The intent is to ensure that the auditor who is leading the cybersecurity audit is equipped with the relevant knowledge and know-how to conduct the audit.

CYBERSECURITY AWARENESS PROGRAMME

Feedback

14.6. Respondents sought clarification on the frequency of the review of the cybersecurity awareness programme.

CSA's Response

14.7. CSA has revised the clause to provide clarity with regards to the frequency of review. The cybersecurity awareness programme shall be reviewed at least once every 12 months from the completion of the last review.

Feedback

14.8. Respondents sought guidance on the measurement of adoption of the cybersecurity awareness programme within the CII Organisation.

CSA's Response

14.9. CSA has revised the clause for clarity. The intent is to measure the effectiveness of the cybersecurity awareness programme implemented by the CIIO. This measurement would provide the basis for the CIIO to identify gaps for improvements. The CIIO should assess and determine the appropriate measurement to measure the effectiveness of the cybersecurity awareness programme. Examples include quizzes and surveys.

FAMILIARITY WITH CYBERSECURITY LEGISLATIONS

Feedback

14.10. Respondents enquired on the depth of familiarity required on the various Cybersecurity legislations for this section.

CSA's Response

14.11. The CIIO is expected to ensure personnel who use, operate, and manage the CII are aware of the Cybersecurity Act and its subsidiary legislations, code of practices and standards of performance, and understand the cybersecurity policies and legislations pertaining to the use, operate and manage the CII.

15 OT SECURITY REQUIREMENT

OT ARCHITECTURE AND SECURED CODING

Feedback

15.1. Respondents commented on the following:

(a) monitoring the control network may cause a disruption due to its limited bandwidth in the OT network; and

(b) use of unidirectional gateway to send a 1-way data transmission out of CII is secured and there is no threat posed to the CII hence security mechanism for monitoring is not required.

CSA's Response

15.2. The intent is to address the risk of data exfiltration from OT CII. It is important that CIIO monitors the data flow from OT CII to any enterprise network for anomalies and trigger an alert for investigation in the event such anomalies are detected.

15.3. Unidirectional gateway is an effective means to prevent a threat actor breaking into the OT CII network, but it does not address the risk of data exfiltration. As such, monitoring is required.

Feedback

15.4. Respondents sought clarification on how would operational mechanisms mitigate cyber-attacks given that these mechanisms are usually related to safe operations and maintenance.

CSA's Response

15.5. Operational mechanisms do not prevent cyber-attacks but to mitigate consequences from cyber-attacks. For example, they can function as fail-safes to ensure the safety and reliability of operations in the event of a cybersecurity incident.

Feedback

15.6. Respondents sought clarification on the following:

(a) the types of physical processes; and

(b) the rationale of separating Safety Instrumental System (SIS) from other control systems.

CSA's Response

15.7. CSA has defined the physical processes with examples under the OT section.

15.8. CSA has revised the clause for clarity. The intent is to protect the SIS and its functions from being compromised in the event of a cybersecurity incident affecting other computers or computer systems.

Feedback

15.9. Respondents requested for the following:

(a) limit the type of physical processes to critical physical processes;

(b) guidance on what constitutes significant period of operation time in the physical processes; and

(c) examples of physical processes with significant period of operation time.

CSA's Response

15.10. Critical physical processes are dependent on related physical processes within the OT CII. Limiting the scope to critical physical processes will limit triage response time and affect business delivery when the related physical processes are affected by a cyber breach.

15.11. CSA has revised the clause to provide clarity. In the revised clause, significant period of operation time is no longer a criteria. A CIIO will need to identify physical processes controlled by the OT CII and perform the activities stated in the clause, to the extent possible.

Feedback

15.12. Respondents sought clarification whether sharing network devices with logical separation is sufficient to fulfil its compliance to the segregation of OT network.

CSA's Response

15.13. The intent is to ensure the OT CII network is physically segregated from the enterprise network. This is to prevent threat actors from pivoting from the enterprise network into the OT CII network. As such, sharing of network devices between OT CII network and enterprise network is not allowed.

Feedback

15.14. Respondents commented that cybersecurity auditors are not certified nor have the necessary experience to audit plant processes or plant safety.

CSA's Response

15.15. The CIIO should first be satisfied with the competency and experience of the proposed auditors to provide an independent and objective assessment of the effectiveness of the CII processes and controls in the OT environment prior to submitting the list of proposed auditors to CSA for approval.

Feedback

15.16. Respondents commented that OEM supports are required to prevent baseline deviation and the processes/programme code are proprietary. In addition, preventing deviation may not be feasible due to the dynamic of the operation.

CSA's Response

15.17. The clause has been revised for clarity. Preventing deviation is not the intent. The intent is to monitor deviation to ensure that the CIIO tracks the deviation and triggers an alert for investigation. CSA also noted that the CIIO will require OEM's support and encourage the CIIO to work closely with OEM to ensure deviation can be detected promptly.

Feedback

15.18. Respondents sought guidance on how to validate the input value to the field controller.

CSA's Response

15.19. The intent for implementation of input validation mechanism within the programme code for the field controller is to ensure out-of-bound checks for valid operational values as well as valid values in term of data types that are relative to the process. An example could be cross-checking set-point input value of 101 within a valid operational range (i.e. 0-100) in the field controller will flag an illegal process, and the value of 101 will not be processed.

Feedback

15.20. Respondents sought clarification on the requirements to assign data and function registers within the field controller.

CSA's Response

15.21. CSA has revised the clause for clarity. The intent for assigning distinct read and write registers blocks for specific functions is to validate data, avoid buffer overflows and block unauthorised writes to protect controller data. Any temporary memory (unassigned) is an easily exploitable area of memory that could lead to memory register being overwritten due to malicious attempt that will disrupt an operation.

Feedback

15.22. Respondents enquired on the rationale to modularise programme codes.

CSA's Response

15.23. The intent is to facilitate testing and keeping track of the integrity of programme code modules. If the programme code insides the module has been tested, any modifications to these modules can be verified against the hash of the original programme code. This way, modules can be validated if the integrity of the code is in question after an incident.

Feedback

15.24. Respondents also enquired on what is the intent of identifying and documenting programme codes that require a fail-safe state.

CSA's Response

15.25. The intent is to prioritise human safety and minimise disruption to the OT CII. In the event of a disruption, the OT CII can transit to a safe and desired state.

Feedback

15.26. Respondents sought clarification on the following:

(a) definition of a field controller in the OT environment;

(b) the definition of cycle time, operational uptime, stop state or memory usage; and

(c) the required frequency for monitoring anomalies.

CSA's Response

15.27. Field controller is defined in the glossary section as an industrial computer (e.g. PLC, RTU, etc) in an OT environment used to monitor and/or control physical processes.

15.28. The system parameters' values on a field controller are usually in steady state unless there are changes to its environment, process or programme code. These are typical system variables found within the field controller that can be used to summarise times used to detect significant changes. For example, the system variable (i.e. cycle time) will increase when an attacker added malicious code to the field controller.

15.29. The monitoring process should be continuous. The intent is to monitor for deviations and anomalous activities and to trigger alerts for investigation when such events are detected.

Feedback

15.30. Respondents commented that monitoring the parameters (cycle time, operational uptime, stop-state and memory usage) does not assist in detecting a cyber incident and suggested that monitoring via operational trends could be more relevant as it is very hard or near impossible for an attacker to modify the field controller.

CSA's Response

15.31. Monitoring the parameters could help in assisting the detection of a cybersecurity incident. For example, the cycle time parameter can be summarised and sent to the HMI for trending. An alert should be triggered for investigations if the trend line deviates from the baseline of normal operation.

Feedback

15.32. Respondents suggested to review the baseline of normal operation of field controller at least once every 24 months as opposed to 12 months because it can be challenging to review the field controllers in different geographically locations.

CSA's Response

15.33. CSA noted the potential challenges to review field controllers' baseline of normal operation where they are distributed in different locations. As the OT cyber threat landscape is evolving rapidly, the CIIO needs to continue to monitor and reassess their cyber risk environment on a timely basis to stay relevant against the cyber threat faced. The CIIO is required to review the baseline of normal operation, at least once every 12 months, from the completion of the last review.

CONNECTIONS TO FIELD CONTROLLER

Feedback

15.34. Respondents sought clarification on the following:

(a) definition of "data interface" for the field controllers;

(b) the rationale of using dedicated communication module and equipment; and

(c) the rationale of restricted array of data to connect to third-party data interface.

CSA's Response

15.35. CSA has revised the clause for clarity. The data interface refers to the third-party interface that field controller is connecting to.

15.36. CSA has revised the clause for clarity. The intent is to reduce cybersecurity risks for field controllers connecting to any external network or device. As such, the CIIO is required to establish a separate communication module when connecting to any external network or device to prevent unauthorised access to the OT CII through the field controller.

15.37. The clause has been revised for clarity. The intent is to prevent unauthorised data transmission, including unauthorised write functions to ensure the safety and reliability of the operations.

Feedback

15.38. Respondents also requested for guidance on the following:

(a) authentication for logging onto field devices (i.e. transmitter/valve); and

(b) the requirement for enabling security feature on the field controller.

CSA's Response

15.39. The intent is to implement authentication process for data transmission between the field controller and any network or device, instead of electrical interfaces or electrical/mechanical equipment.

15.40. The intent is to protect the field controllers from cybersecurity threats. As such, the CIIO is required to work with their vendors and/or OEM to enable recommended security feature(s) that is/are available in the field controllers. For example, enabling password protection to prevent unauthorised access.

With Thanks To

CSA wishes to acknowledge the contributions from the following stakeholders. Your feedback has helped CSA to make the CCoP 2.0 better.

Forty-three (43) CII public and private organisations across the eleven (11) CII sectors. Agency/Company names are not published for operations security reasons.

Trade Association

Access Partnership
AIG APAC Holdings
AmCham Singapore
Amazon
Apple
Avanade Asia
Baker & McKenzie
BSA | The Software Alliance
Cisco Systems
Google Cloud, Asia Pacific
Honeywell Technology Solutions
IBM Singapore
Johnson Controls S
JP Morgan Chase
K&C Protective Technologies
Keysight Technologies
Lubrizol Southeast Asia
Mandiant Singapore
Marsh (Singapore)
Mesh Bio
Meta
Microsoft Singapore
PayPal
Raytheon Technologies
SAP Asia
Seagate Singapore International Headquarters
Splunk
US-ASEAN Business Council
Vriens & Partners

Industry

Abbott Laboratories (Singapore)
AcuiZen Technologies Singapore
ACE
Amadeus
American Express
Asia Cloud Computing Association
Assure IT Pte. Ltd.
ASTM International
ATvanGarde
Becton Dickinson & Co
ComfortDelGro Corporation
Deloitte
ECV Holdings
Ensign InfoSecurity (SmartTech)
Ernst & Young Advisory Singapore
Honeywell Connected Enterprise
HP Singapore
IBM Singapore
ISACA Singapore
JP Morgan
Keppel Infrastructure Holdings
KPMG Singapore
Maximus Consulting
McLarty Associates
Microsoft Singapore
MSD International GmbH (Singapore Branch)
Nathan Associates
NETS Pte Ltd
Novartis Singapore
NTT Singapore
Palo Alto Networks
Pulse Secure
PwC
Salesforce
Sapience Consulting
SOCOTEC Certification Singapore
SRMS Asia
U.S. Embassy
US-ASEAN Business Council

Verizon Business Group - Global Security Services
Visa Worldwide