GUIDELINES FOR AUDITING CRITICAL INFORMATION INFRASTRUCTURE

JANUARY 2020

CONTENTS

1 INTRODUCTION

Under section 15(1)(a) of the Cybersecurity Act 2018 ("The Act"), the owner of a Critical Information Infrastructure ("CIIO") must, starting from the date of the notice issued under section 7 (Designation of CII), cause a cybersecurity audit of the compliance of the CII with the Act and applicable codes of practice ("CoPs") and standards of performance ("SoPs").

The cybersecurity audit must be carried out at least once every two years (or at such higher frequency as may be directed by the Commissioner of Cybersecurity in any particular case), and to be carried out by an auditor approved or appointed by the Commissioner.

2 PURPOSE

The purpose of this document is to set the audit expectations, and to serve as a guide for approved or appointed auditors to conduct cybersecurity audit and COI audit (Implementation of SingHealth's Committee of Inquiry ("COI") recommendations) of CIIs.

This document is not meant to be an exhaustive source of information for conducting a CII cybersecurity audit. In the absence of any cybersecurity audit topics not covered in this guide, the auditor should exercise their professional judgement and highlight such situation in the audit report.

3 AUDIENCE

The intended audience of this document includes, but not limited to, the following:

a. Auditors who have been formally approved or appointed by the Commissioner; and

b. Stakeholders (E.g. business unit heads, system owners and vendor, Chief Information Security Officers, etc.) who need to know about the cybersecurity audit expectations for auditing their CII.

4 SCOPE

This document covers the following cybersecurity audits:

a. The cybersecurity audit under the Act. Refer to Section 6: AUDIT EXPECTATIONS; and

b. An additional audit covering the COI audit. Refer to Section 7: COI AUDIT.

5 AUDITOR APPROVAL

Auditors have to be approved or appointed by the Commissioner to conduct cybersecurity audit on the CII. To complete the application for Commissioner's approval, both the CIIOs and auditors are required to submit the relevant forms[1] as specified by CSA. While the auditors can directly submit the applicable form to CSA, the application would only be deemed complete after all the relevant forms and accompanying documents submitted by the CIIOs and auditors are complete and in order.

There are two main criteria, i.e. independence and competency, that the proposed audit firm/team and auditors need to fulfil. The appointed audit firm/team and auditors:

a. Should not be in a position of any conflict of interest, whether actual, potential or perceived. A conflict of interest refers to any circumstance where the auditor's interests may potentially interfere with the independent and objective performance of his/her duties as an auditor; and

b. Should possess the necessary technical competencies (i.e. professional qualifications/ certifications, skills, knowledge and relevant experiences) to perform the audits.

[1] The auditor approval forms can be obtained from the CIIOs.

6 AUDIT EXPECTATIONS

This section sets out CSA's audit expectations. It is intended to help the reader understand how cybersecurity audit should be conducted and reported.

CSA has listed down seven areas of audit expectations in sections 6.1 to 6.7.

6.1 Principles of Auditing

Audits should adhere to the following principles for providing relevant and sufficient audit conclusion. This is to enable auditors, working independently, to reach similar conclusions in similar circumstances.

a. **Integrity**: The foundation of professionalism.
   - Perform audits with honesty and responsibility.
   - Ensure competence while performing audits.
   - Perform audits in an impartial manner.
   - Ensure fair and unbiased in all dealings. Be sensitive to any influences that may be exerted on auditor's judgement during an audit.

b. **Fair Presentation**: The obligation to report truthfully and accurately.
   - Ensure audit findings, audit conclusions and audit reports reflect truthfully and accurately the audit activities.

- Report significant obstacles encountered during audit and unresolved diverging opinions between the audit team and the auditee.
- Ensure the communication is truthful, accurate, objective, timely, clear and complete.

c. **Due Professional Care**: the application of diligence and judgement in auditing.
   - Exercise due care in accordance with the importance of the task and the confidence placed in auditor by the audit client and other interested parties.
   - Make reasoned judgements in all audit situations.

d. **Confidentiality**: Security of information.
   - Exercise discretion in the use and protection of information obtained during audit.
   - Do not use the audit information for personal gain or in detrimental way to the legitimate interests of the auditee.
   - Handle sensitive or confidential information properly.

e. **Independence**: The basis for the impartiality of the audit and objectivity of the audit conclusions.
   - Ensure independence of the activity being audited.
   - Act in a manner that is free from bias and conflict of interest in all cases.
   - Maintain objectivity throughout the audit process.
   - Ensure the audit findings and conclusions are based only on the audit evidence.

6.2 Audit Objective

The objective of the audit is to:

a. Verify the compliance of CII against requirements stipulated in Part 3 of the Act, including the subsidiary legislation, applicable written directions, CoPs and SoPs; and

b. Assess the adequacy and effectiveness of controls/measures put in place to meet the requirements stipulated in Part 3 of the Act, including the subsidiary legislation, applicable written directions, CoPs and SoPs.

6.3 Audit Scope

The audit shall cover the following:

Scope	Description
Audit Subject	The audit subject should cover all CII that has been designated under the Act.
Audit Period	The audit period should minimally be 12 months and there should be no gap between the audit periods for each CII.
Audit Criteria	The audit criteria should include compliance with the Act, subsidiary legislation, applicable written directions, CoPs, and SoPs. If a waiver is granted, the CoP clause remains subjected for cybersecurity audit as pursuant to section 15(1)(a) of the Act. The auditor should check the validity of the justification, the waiver condition and the effectiveness of the compensating controls.

6.4 Audit Approach

The audit should adopt both a compliance and risk-based approach.

a. Compliance-based
   Carry out compliance test to ascertain the adequacy and effectiveness of the controls applied in the CII to comply with the Act, subsidiary legislations, applicable written directions, CoP, and SoP.

b. Risk-based
   Identify the risks and threats that the CII faces and ascertain if the controls put in place are appropriate to mitigate the known risks and threats.

6.5 Audit Finding

The auditor should highlight the following:

a. Any audit finding identified during the course of the audit;

b. Highlight systemic finding, where the finding is spread throughout the CII, which could likely be a weakness in the design of the control;

c. Highlight recurring finding, i.e. finding brought up from past audits that have re-occurred in the current audit even after implementing the corrective action; and

d. Highlight good practices, in areas of governance and controls, noted during the course of the audit.

When raising an audit finding, the auditor should clearly articulate the following attributes of the audit finding.

Attributes	Description
Condition	Statement that describes the results of the audit finding.
Criteria	Standards/ Rules/ Benchmarks (e.g. Cybersecurity Act, policies and best practices) used to measure against the condition.
Cause	The root cause and contributory reason(s) for the condition.
Effect	The effect and significance of the condition (Immediate, future or potential). The auditor should associate the audit finding to the impact on CII's essential services in which the management is familiar with, i.e. quantitative effect (e.g. cost, time and production) and qualitative effect (e.g. service and poor decision-making). This helps to convince the management on the need for corrective action.
Recommendation	Recommend action(s) to correct the cause to prevent the reoccurrence of the audit finding.

6.6 Audit Conclusion

The auditor should give their opinion and conclusion on the following areas:

a. Appropriateness of the management comments in response to the audit finding;

b. Adequacy and effectiveness of the controls put in place by the CIIO to address cybersecurity risks to the CII; and

c. Opportunities for improvement to secure the CII.

6.7 Audit Report Format

The audit report should minimally contain the following:

Content	Description
Executive Summary	The report should provide an overall evaluation of the findings noted, with a description of the issues, cybersecurity risks and potential implications on the CII, recommendations, management comments, and the auditor's assessment of the appropriateness of the management comments. The executive summary should also include the auditor's conclusion on the overall adequacy and effectiveness of controls in addressing the cybersecurity risks to the CII.
Purpose	The report should describe the purpose of conducting the cybersecurity audit (e.g. to fulfil obligations under Cybersecurity Act, to fulfil ad-hoc directions given by Commissioner, etc).
Audit Objective	Audit objective is defined in section 6.2 of this document.
Audit Scope	Audit scope is defined in section 6.3 of this document.
Stakeholders	The stakeholders involved in the cybersecurity audit and their roles and responsibilities should be clearly stated in the report.
Audit Methodology and Approach	The report should provide an explanation of how the cybersecurity audit was performed to meet the audit objectives. Specifically, the explanation should state: a. Whether the work of other auditors (e.g. past audits) or cybersecurity assurance practitioner was relied upon and the extent to which such reliance was made; b. The types of analysis and techniques used to perform the audit (e.g. interviews, walkthroughs, document inspection); and c. Sampling methods adopted (if samples are chosen to assess effectiveness of controls).
Audit Finding	Audit finding is defined in section 6.5 of this document.
Audit Conclusion	Audit conclusion is defined in section 6.6 of this document.

7 COI AUDIT

7.1 Background

Following the cyber-attack on SingHealth, a COI was convened to inquire into the events and contributing factors leading to the cyber-attack. The COI had made 16 recommendations to enhance organisations' capability to deter, detect, respond to and recover from cybersecurity incidents and the Government accepted all of the recommendations.

The aim of the recommendations are to:

a. Strengthen organisational structure
b. Raise staff cybersecurity competencies
c. Improve system and data protection
d. Enhance security checks on systems
e. Improve incident response processes

7.2 Purpose

In October 2019, Minister-in-charge of Cybersecurity, S. Iswaran instructed that an independent audit should be carried out to validate the implementation of SingHealth COI recommendations on all the CIIs.

7.3 COI Audit Expectations

The COI audit expectations are listed in the table below.

Audit Expectations	Description
Audit Objective	The objective of the audit is to: a. Validate the implementation status of the COI recommendations; and b. Ascertain the adequacy and effectiveness of the implemented controls, including the interim and compensating controls put in place to address the risks mentioned in the COI report.
Audit Scope	<u>Audit Subject & Audit Period</u> Audit subject and audit period are defined in section 6.3 of this document. <u>Audit Criteria</u> The audit criteria should cover the latest submission[2] to CSA by the CIIO on the follow-up status of COI recommendations.

[2] The auditor should obtain the latest submission from the CIIO prior to the commencement of the audit.

Audit Expectations	Description
Audit Completion Timeline	The COI audit should be completed by 31 December 2020 and the audit report should be submitted to CSA not later than 30 days after the completion of the audit.
Audit Approach	Audit approach is defined in section 6.4 of this document.
Audit Finding	Audit finding is defined in section 6.5 of this document.
Audit Conclusion	Audit conclusion is defined in section 6.6 of this document.
Audit Report Format	Audit report format is defined in section 6.7 of this document.

7.4 COI Audit Deliverables

Apart from delivering the COI audit report in the format defined in section 6.7 of this document, the auditor should also complete an audit worksheet titled "*Implementation of COI Recommendations - Audit Template*"[3] and submit it together with the audit report.

[3] The audit worksheet can be obtained from the CIIOs.

8 TERMS AND DEFINITIONS

For the purpose of this document, the following terms and definitions apply.

SN	Term	Definition
8.1	Audit	The systematic, independent and documented process for obtaining audit evidence (SN 8.3) and evaluating objectively to determine the extent to which the audit criteria (SN 8.2) are fulfilled.
8.2	Audit criteria	A set of requirements used as a reference against which audit evidence (SN 8.3) is compared.
8.3	Audit evidence	Audit evidence refers to records, statements of fact or other information, which are relevant to the audit criteria (SN 8.2) and verifiable.
8.4	Audit finding	An audit criteria not being met.
8.5	Audit period	The period of time to which the audit work relates and from which audit evidence is obtained.
8.6	Audit subject	Audit subject refers to the CII system that is to be audited.
8.7	Adequacy of control	Adequacy refers to whether the control in place is fit for the purpose.
8.8	Compensating control	Compensating control, also called an alternative control, may be considered when an entity cannot meet a requirement explicitly as stated, due to legitimate technical or documented business constraints, but has sufficiently mitigated the risk associated with the requirement through implementation of other controls. Compensating control must: a. Meet the intent and rigor of the original requirement; b. Provide a similar level of defence as the original requirement; and c. Commensurate with the additional risk imposed by not adhering to the requirement.
8.9	Effectiveness of control	Effectiveness refers to whether the control in place has the desired effect of mitigating the risk.

SN	Term	Definition
8.10	Interim control	A set of measures designed to reduce the risk temporarily while the recommended control is being implemented.

9 REFERENCES

[1] ISO 19011:2018(E), "Guidelines for auditing management systems," ISO, 2018.

[2] PCI Security Standards Council, "PCI DSS and PA-DSS Glossary of Terms, Abbreviations, and Acronyms," April 2016. [Online]. Available: https://www.pcisecuritystandards.org/documents/PCI_DSS_Glossary_v3-2.pdf?agreement=true&time=1577691345202. [Accessed 30 December 2019].

[3] ISACA IT Standards, Guidelines, and Tools and Techniques for Audit and Assurance and Control Professionalism, ISACA, 2010.

[4] ISACA Information Systems Auditing: Tools and Techniques - Creating Audit Program, ISACA, 2016.

QUERIES & FEEDBACK

Questions and feedback on this document may be submitted to:

CII_Supervision@csa.gov.sg