SS 712:2025
(ICS 35.020; 35.030)

SINGAPORE STANDARD

Tiered cybersecurity standards for organisations

Singapore Standards Council

SS 712:2025
(ICS 35.020; 35.030)

SINGAPORE STANDARD

Tiered cybersecurity standards for organisations

Published by Enterprise Singapore

ISBN 978-981-5338-53-9

Contents

Foreword

This Singapore Standard (SS) was prepared by the Working Group on Tiered Cybersecurity Standards for Organisations set up by the Technical Committee on Security and Privacy under the purview of the Information Technology Standards Committee (ITSC).

This standard was developed as a result of the review of TR 106:2022, “Tiered cybersecurity standards for enterprises”.

The key changes include:

- Coverage of additional digital technologies to provide digital-technology specific protection for organisations that are implementing cloud computing, Operational Technology (OT) and Artificial Intelligence (AI);

- Updates to protection measures to factor in key changes in the technological landscape, such as AI-enabled threats;

- Updates to library of risk scenarios in the guided risk assessment for trust mark to include scenarios specific to cloud security, OT security and AI security;

- Multi-factor authentication (MFA) – Updated from mark of cyber hygiene “recommendation” to “requirement” to factor in shifts in work arrangements in organisations, and to provide additional protection given how credentials compromise tend to be common entry points into organisations;

- Bring your own device (BYOD) – Extension of existing mark of cyber hygiene requirements on protection of business-critical data to explicitly include BYOD devices, and the incorporation of protective measures that start from trust mark Promoter tier instead of Performer tier;

- Cybersecurity of third parties – Included as mark of cyber hygiene “recommendations” and incorporation of protective measures that start from trust mark Promoter tier instead of Advocate tier to reflect the increase in concerns on the amplified impact as a result of cybersecurity breach in the supply chain;

- Logging – Updated from mark of cyber hygiene “recommendation” to “requirement” to facilitate detection, analysis and recovery; and

- Secure Software Development Life Cycle (SDLC) – Incorporation of protective measures that start from trust mark Promoter tier instead of Advocate tier to reflect the increase in concerns on the amplified impact as a result of cybersecurity breach in the supply chain.

This standard provides tiered cybersecurity measures for organisations of different risk profiles. The mark of cyber hygiene is intended to encourage organisations to establish appropriate cybersecurity controls to protect against common attacks. The trust mark recognises organisations that have implemented good cybersecurity measures. The trust mark also serves as a pathway for organisations to adopt international cybersecurity standards, such as:

- IEC 62443 for industrial security;
- ISO/IEC 27001:2022 for information security;
- ISO/IEC 27017:2015 for cloud security;
- ISO/IEC 42001:2023 for responsible AI[1].

[1] The trust mark primarily focuses on the security of AI usage within the organisation, which is part of a broader set of considerations for responsible AI.

In preparing this standard, reference was made to the following publications:

1. IEC 62443 series on security of industrial automation and control systems
2. ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection – Information security management systems – Requirements
3. ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection – Information security controls
4. ISO/IEC 27017:2015 Information technology – Security techniques – Code of practice for information security controls based on ISO/IEC 27002 for cloud services
5. ISO/IEC 42001:2023 Information technology – Artificial intelligence – Management system
6. Baseline cyber security controls for small and medium organisations V1.2 by Canadian Centre for Cyber Security
7. CIS controls v8 by Centre for Internet Security (CIS)
8. CIS controls v8 cloud companion guide by CIS
9. CIS password policy guide by CIS
10. CISA cyber resilience review (CRR) by Cybersecurity & Infrastructure Security Agency and Carnegie Mellon University's Software Engineering Institute, CERT Division
11. Cyber Essentials and Cyber Trust mark (2022) by Cyber Security Agency of Singapore
12. Cyber Essentials by UK National Cyber Security Centre
13. Cyber risks associated with generative artificial intelligence by Monetary Authority of Singapore (MAS)
14. Cybersecurity assessment tool by Federal Financial Institutions Examination Council
15. Cybersecurity maturity model certification by U.S. Department of Defence
16. Cybersecurity playbook for large language model (LLM) applications by Government Technology Agency
17. Essential Eight by Australian Cyber Security Centre
18. Federal Risk and Authorization Management Program (FedRAMP) by U.S. General Services Administration
19. HITRUST by Health Information Trust Alliance
20. NIST SP 800-82r3 Guide to operational technology (OT) security by National Institute of Standards and Technology (NIST)
21. Payment card industry data security standard (PCI DSS) by Visa, MasterCard, Discover Financial Services, JCB International and American Express
22. System and Organization Controls (SOC) for service organisations by American Institute of Certified Public Accountants
23. Technology risk management guidelines by MAS
24. The five ICS cybersecurity critical controls by SANS Institute
25. The NIST cybersecurity framework (CSF) 2.0 by NIST

Acknowledgement is made for the use of information from the above publications.

Permission has also been sought from the Cyber Security Agency of Singapore for the reproduction of materials from their publications into this standard:

1. SG Cyber Safe Programme – Cyber Essentials mark
2. SG Cyber Safe Programme – Cyber Trust mark

NOTE

1. *Singapore Standards (SSs) and Technical References (TRs) are reviewed periodically to keep abreast of technical changes, technological developments and industry practices. The changes are documented through the issue of either amendments or revisions. Where SSs are deemed to be stable, i.e. no foreseeable changes in them, they will be classified as "mature standards". Mature standards will not be subject to further review unless there are requests to review such standards.*

2. *An SS or TR is voluntary in nature except when it is made mandatory by a regulatory authority. It can also be cited in contracts making its application a business necessity. Users are advised to assess and determine whether the SS or TR is suitable for their intended use or purpose. If required, they should refer to the relevant professionals or experts for advice on the use of the document. Enterprise Singapore and the Singapore Standards Council shall not be liable for any damages whether directly or indirectly suffered by anyone or any organisation as a result of the use of any SS or TR. Although care has been taken to draft this standard, users are also advised to ensure that they apply the information after due diligence.*

3. *Compliance with a SS or TR does not exempt users from any legal obligations.*

Tiered cybersecurity standards for organisations

0 Introduction

The digital landscape is evolving at an unprecedented rate and offers vast and diverse opportunities for all. However, this digital transformation also increases organisational and individual exposure to cyber risks. Building organisations' confidence in managing cyber risks is therefore essential to enable them to protect their valuable assets, harness the opportunities presented by digitalisation and foster consumer trust.

This Singapore Standard outlines tiered cybersecurity standards designed to support the cybersecurity needs of a diverse range of organisations. A framework has been developed to guide organisations in their journey towards implementing effective cybersecurity measures.

1 Scope

Organisations differ in terms of their business nature, size (which may be measured by parameters such as capital turnover or employee count), and the extent of digitalisation within their operations. These factors directly influence their cybersecurity risk profiles. This standard adopts a tiered approach to address these diverse business profiles and needs as follows:

– The mark of cyber hygiene focuses on baseline controls to protect organisations against the most common cyberattacks; and

– The trust mark takes emphasises a risk-based approach, enabling organisations to implement appropriate cybersecurity preparedness measures with their specific cybersecurity risk profiles.

Collectively, the mark of cyber hygiene and trust mark provide a cybersecurity risk management framework for organisations.

The cybersecurity risk management framework outlined in this standard encompasses classical cybersecurity concepts[2], cloud security, operational technology (OT) security and artificial intelligence (AI) security. This is intended to reflect how cybersecurity is not static, but a dynamic field that constantly evolves as organisations adopt[3] and utilise technology with increasing intensity[4].

2 Normative references

There are no normative references in this standard.

[2] Typically refers to the measures that secure and protect information technology (IT) assets.
[3] Refers to percentage of organisations adopting at least 1 digital technology in Singapore Digital Economy 2023 report published by Infocomm Media Development Authority (IMDA) and Lee Kuan Yew School of Public Policy.
[4] Refers to average number of digital technologies adopted per organisation in Singapore Digital Economy 2023 report published by IMDA and Lee Kuan Yew School of Public Policy.