TR 106:2022
(ICS 35.020; 35.030)

TECHNICAL REFERENCE

Tiered cybersecurity standards for enterprises

Singapore Standards Council

TR 106:2022
(ICS 35.020; 35.030)

TECHNICAL REFERENCE

Tiered cybersecurity standards for enterprises

Published by Enterprise Singapore

ISBN 978-981-5073-42-3

Contents

Foreword

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

This TR provides tiered cybersecurity measures for enterprises of different risk profiles. The mark of cyber hygiene is intended to nudge enterprises to put in place appropriate cybersecurity controls to protect against common attacks. The trust mark is a mark of distinction to recognise enterprises that have put in place good cybersecurity measures. The trust mark also serves as a pathway for enterprises to adopt international cybersecurity standards (e.g., ISO/IEC 27001).

This TR is a provisional standard made available for application over a period of three years. The aim is to use the experience gained to update the TR so that it can be adopted as a Singapore Standard. Users of the TR are invited to provide feedback on its technical content, clarity, and ease of use. Feedback can be submitted using the form provided in the TR. At the end of the three years, the TR shall be reviewed, taking into account any feedback or other considerations, to further its development into a Singapore Standard if found suitable.

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

1. ISO/IEC 27001:2013 Information technology – Security techniques - Information security management systems — Requirements
2. ISO/IEC 27002:2013 Information technology – Security techniques - Code of practice for information security controls
3. Baseline Cyber Security Controls for Small and Medium Organisations V1.2 by Canadian Centre for Cyber Security
4. CIS Controls v8 by Centre for Internet Security
5. CIS Password Policy Guide by Centre for Internet Security
6. CISA Cyber Resilience Review (CRR) by US Department of Homeland Security (DHS) and CERT Division of CMU Software Engineering Institute
7. Cyber Essentials by UK National Cyber Security Centre (NCSC)
8. Cybersecurity Maturity Model Certification (CMMC) by US Department of Defence
9. Essential 8 by Australian Cyber Security Centre
10. Federal Financial Institutions Examination Council (FFIEC) Cybersecurity Assessment Tool
11. Federal Risk and Authorisation Management Programme (FedRAMP) by US federal government
12. HiTrust by Health Information Trust Alliance
13. NIST Cybersecurity Frameworks
14. Payment Card Industry Data Security Standard (PCI DSS) by Visa, MasterCard, Discover Financial Services, JCB International and American Express.
15. SOC for Service Organisations by American Institute of Certified Public Accountants (AICPA)
16. Technology Risk Management Guidelines (TRMG) by Monetary Authority of Singapore (MAS)

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

Attention is drawn to the possibility that some of the elements of this TR may be the subject of patent rights. Enterprise Singapore shall not be held responsible for identifying any or all of such patent rights.

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 enterprises

0 Introduction

Digitalisation creates new opportunities and COVID-19 has accelerated the rise of the digital economy. An increasingly digital way of life also increases organisational and individual exposure to cyber risks. Cybersecurity is a critical enabler of Singapore's digital economy. There is a need to build confidence in organisations to enable them to pursue the opportunities from digitalisation. Cybersecurity incidents often result in financial losses, tarnish business reputation and affect customers' trust, negating business investments and customers' confidence in the digital economy.

This Technical Reference (TR) describes tiered cybersecurity standards that are designed to support the cybersecurity needs of a range of organisations. A framework has been developed to provide a guided approach to help organisations in their journey towards the implementation of cybersecurity in the organisation.

1 Scope

Organisations differ in terms of the nature of their business, size (which may be measured by parameters such as capital turnover or employment size) and the extent of digitalisation in their businesses. These have a corresponding impact on their cybersecurity risk profile. This TR takes on a tiered approach to address different business profiles and needs as follows:

– The mark of cyber hygiene takes on a baseline control approach and is intended to protect organisations against the most common cyberattacks; and

– The trust mark takes on a risk-based approach and is intended to enable organisations to put in place the relevant cybersecurity preparedness measures that commensurate with their cybersecurity risk profile.

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

2 Normative references

There are no normative references in this standard.