

## CSA Cyber Trust mark Certification

As businesses move towards digitalisation to improve operational efficiency, they inevitably become more vulnerable and exposed to cyberattacks. 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, affect business reputation, negating business investments and customers' confidence in the digital economy.

The Cyber Trust mark can be a testament to your organisation's sound cybersecurity practices and measures. It is a certification program developed by the Cyber Security Agency of Singapore (CSA) for organisations with more established digitalisation processes and invested protection for their IT infrastructure. SETSCO's qualified and experienced auditors can conduct objective assessment of your cybersecurity procedures and safeguards to ensure that they meet the Cyber Trust mark requirements developed by CSA and henceforth provide your organisation with greater assurance of being "cyber safe".

The Cyber Trust mark is a cybersecurity certification created for organisations with more extensive digitalised business operations. It is targeted at larger or more digitalised organisations as these organisations tend to have higher risk levels that require investment in expertise and resources to help manage and protect their IT infrastructure and systems. The Cyber Trust mark also adopts a risk-based approach in meeting your organisation's needs without over-investing.

The Cyber Trust mark was updated in April 2025 to go beyond classical cybersecurity. CSA has enhanced the Cyber Trust mark, empowering organisation to address cyber risk not just in traditional IT systems, but also Cloud Security, Operational Technology (OT) Security, and AI Security. This enhancement enables businesses to stay ahead of emerging threats and reinforce digital trust among stakeholders.

### Benefits of attaining the CSA Cyber Trust mark

#### **1. Takes on risk-based approach with over-investing**

The Cyber Trust mark takes on a risk-based approach to guide organisations in identifying gaps in their implementation of the cybersecurity preparedness measures so that their implementation commensurate with their cybersecurity risk profiles.

#### **2. Compliant with Industry Best Practices**

The Cyber Trust mark aligns your organisation with national cybersecurity standards and frameworks. It also enables you to keep abreast with the latest industry practices and guidelines while ensuring that your security controls are effective and up-to-date.

#### **3. Enhanced Stakeholder Trust**

The Cyber Trust mark is an endorsement of your organisation's commitment to cybersecurity. It instils confidence in your stakeholders (including clients, partners and customers) that their data and sensitive information are protected.

#### 4. Competitive Advantage

With the Cyber Trust mark, it differentiates you from your competitors and helps your organisation position itself as a trusted and reliable partner. It demonstrates your commitment to cybersecurity, giving you a competitive edge in the market.

#### 5. Provides a pathway to ISO/IEC 27001 certification

The Cyber Trust mark provides a pathway to International standards such as ISO/IEC 27001.

Organisation who wish to assess against ISO/IEC 27001 may refer to the mapping in [CSA](#) website, which maps the cybersecurity preparedness statements in Cyber Trust mark to ISO/IEC 27001.

## Frequently Asked Questions

### For how long is the Cyber Trust mark certificate valid?

The certification is valid for a duration of 3 years, with yearly audits.

### Certification Fee and Funding Support

Cyber Trust (2025) Certification Fee						
Quantity of End-Points	Classical Cybersecurity		Add-on Digital Technologies			
	Classical Cybersecurity	Maximum Level of Support from CSA	Cloud Security	OT Security	AI Security	Maximum Level of Support from CSA
<b>1 – 10</b>	\$1,600 - \$4,600	\$1,375	+ \$350	-	+ \$350	\$225
<b>11 – 20</b>	\$4,700 - \$8,600	\$1,375	+ \$400	-	+ \$400	\$225
<b>21 – 50</b>	\$5,100 - \$9,100	\$1,625	+ \$400	-	+ \$400	\$225
<b>51 – 100</b>	\$5,600 - \$9,600	\$1,875	+ \$500	-	+ \$500	\$225
<b>101 – 200</b>	\$6,100 - \$10,100	\$2,250	+ \$500	-	+ \$500	\$450
<b>201 – 500</b> <i>(in increments of 100 end-points)</i>	\$7,600 - \$12,600	<i>Funding support is available up to 1<sup>st</sup> 200 end-points only.</i>	+ \$500	-	+ \$500	<i>Funding support is available up to 1<sup>st</sup> 200 end-points only.</i>
<b>501 and above</b> <i>(in increments of 100 end-points)</i>	\$8,100 - \$14,600		+ \$350	-	+ \$350	

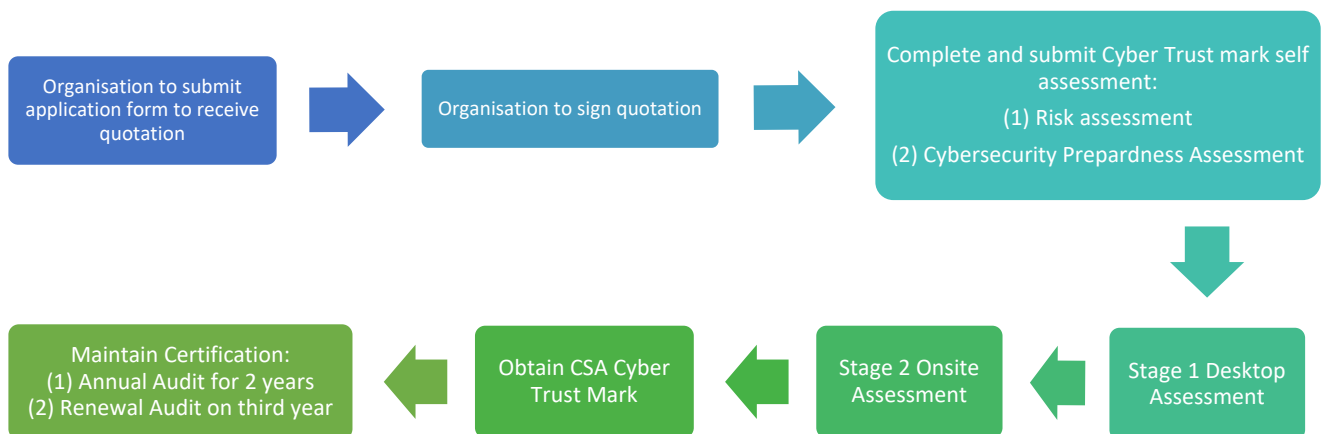
Cyber Trust (2022) Certification Fee			
Quantity of End-points	Certification Fee for Cyber Trust mark	Maximum Level of Support from CSA (First Successful Application)	Certification Fee Charged to Industry (Factoring in CSA Support)
1 – 10	\$1000 - \$4000	\$500	\$500 - \$3500
11 – 20	\$4000 - \$8000	\$725	\$3275 - \$7275
21 – 50	\$4000 - \$8000	\$850	\$3150 - \$7150
51 – 100	\$4000 - \$8000	\$1350	\$2650 - \$6650
101 – 200	\$4000 - \$8000	\$1600	\$2400 - \$6400

### Funding Support

- Applicable for first time application only
- Only Singapore registered businesses and Non-Profit Organisations (NPO) incorporated in Singapore are eligible

For more information on the fund support, please visit [CSA](#) website

### Application process



- Assessment involves both the review and verification of documents, as well as implementation and effectiveness
- Organisations should ensure that they have approximately three (3) months of implementation data/logs in their systems prior to assessors performing verification of implementation and effectiveness

## Which cybersecurity preparedness tier does my organisation belong to?

There are five Cybersecurity Preparedness tiers, with 10 to 22 domains under each tier. Organisations can use the Cyber Trust mark risk assessment framework to identify which Cybersecurity Preparedness Tier is most suited to their needs.

	<b>Tier 1: Supporter</b>	<b>Tier 2: Practitioner</b>	<b>Tier 3: Promoter</b>	<b>Tier 4: Performer</b>	<b>Tier 5: Advocate</b>
<b>Cyber Governance and Oversight</b>					
1. Governance			•	•	•
2. Policies and procedures			•	•	•
3. Risk management	•	•	•	•	•
4. Cyber strategy					•
5. Compliance	•	•	•	•	•
6. Audit				•	•
<b>Cyber Education</b>					
7. Training and awareness*	•	•	•	•	•
<b>Information Asset Protection</b>					
8. Asset management*	•	•	•	•	•
9. Data protection and privacy*	•	•	•	•	•
10. Backups*	•	•	•	•	•
11. Bring Your Own Device (BYOD)			•	•	•
12. System security*	•	•	•	•	•
13. Anti-virus/Anti-malware*	•	•	•	•	•
14. Secure Software Development Life Cycle (SDLC)			•	•	•
<b>Secure Access and Environment</b>					
15. Access control*	•	•	•	•	•
16. Cyber threat management				•	•
17. Third-party risk and oversight			•	•	•
18. Vulnerability assessment			•	•	•
19. Physical/environmental security		•	•	•	•
20. Network security		•	•	•	•
<b>Cybersecurity Resilience</b>					
21. Incident response*	•	•	•	•	•
22. Business continuity/disaster recovery		•	•	•	•
	<b>10 DOMAINS</b>	<b>13 DOMAINS</b>	<b>19 DOMAINS</b>	<b>21 DOMAINS</b>	<b>22 DOMAINS</b>
*Measures in Cyber Essentials mark					