Cyber Trust Mark

The **Cyber Trust** mark is a cybersecurity certification for organisations with more extensive digitalised business operations. It serves as a mark of distinction for your organisation to prove that you have put in place good cybersecurity practices and measures that are commensurate with your cybersecurity risk profile.

Why should my organisation apply?

- Signifies a mark of distinction to recognise organisations as trusted partners with robust cybersecurity
- Provides pathway to international cybersecurity standards (e.g. ISO/IEC 27001)
- Provides a guided approach for your organisation to assess cybersecurity risks and preparedness
- Takes on a risk-based approach to meet your organisation's needs without over-investing

Demonstrate that you are a trusted business partner.

Scan to learn more:

Which tier of Cybersecurity Preparedness 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 more suitable for their needs.

	Tier 1: Supporter	Tier 2: Practitioner	Tier 3: Promoter	Tier 4: Performer	Tier 5: Advocate
Cyber Governance and Oversight					
1. Governance			•	•	•
2. Policies and procedures			•	•	•
3. Risk management	•	•	•	•	•
4. Cyber strategy					•
5. Compliance	•	•	•	•	•
6. Audit				•	•
Cyber Education					
7. Training and awareness*	•	•	•	•	•
Information Asset Protection					
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)					•
Secure Access and Environment					
15. Access control*	•	•	•	•	•
16. Cyber threat management				•	•
17. Third-party risk and oversight					•
18. Vulnerability assessment			•	•	•
19. Physical/environmental security		•	•	•	•
20. Network security		•	•	•	•
Cybersecurity Resilience					
21. Incident response*	•	•	•	•	•
22. Business continuity/disaster recovery		•	•	•	•
	10 DOMAINS	**13 DOMAINS**	**16 DOMAINS**	**19 DOMAINS**	**22 DOMAINS**

*Measures in Cyber Essentials mark

CSA SINGAPORE

SG CYBER SAFE | CYBER TRUST