CSA SG Cyber Safe – Cyber Trust Mark

Why should my organization apply?

Benefits of CSA Cyber Safe Cyber Trust Mark

- Signifies a mark of distinction to recognize enterprises as trusted partners with robust cybersecurity
- Increased reliability and security of systems and information
- Improve customer and business partner confidence
- Increased business resilience
- Be recognized as a trusted brand
- Minimize your legal threats exposure, thus minimizing the risk of getting fined
- Provides a pathway to international standards such as ISO/IEC 27001 and other schemes related to the IoT and Cybersecurity
- Provides a guided approach for your organization to assess cybersecurity risks and preparedness
- Adopt a risk-based approach to meet your enterprise needs without over-investing

What is the Certification Duration valid for Cyber Trust Mark?

The Cyber Trust certification is valid for 3 years, with an annual audit.

CSA SG Cyber Safe Cyber Trust mark – Pricing Table

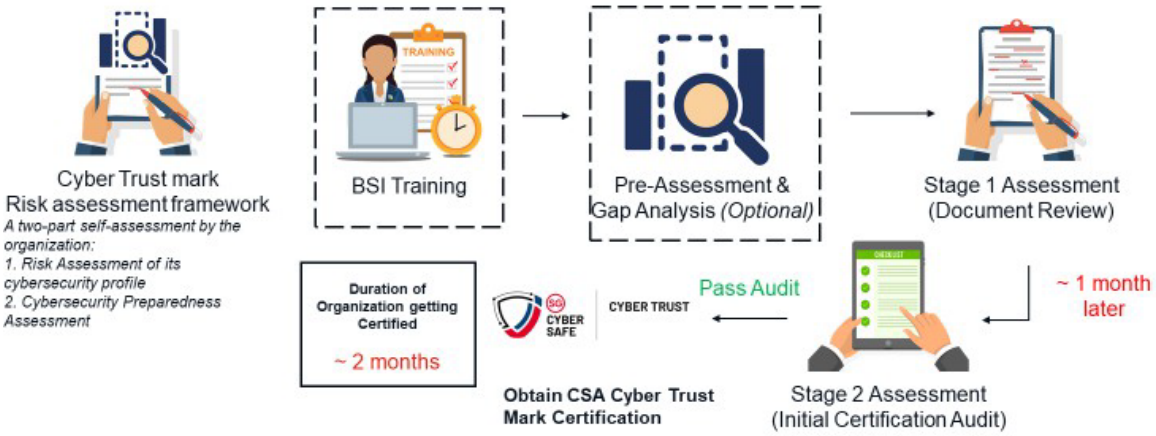
The table below illustrates the indicative price range for the first year's audit (stage 1 and 2).

Quantity of End-points	**Range of Certification Fee Charged**		**Maximum Level of Support from CSA**	**Certification Fee Charged to Industry** (Factoring in CSA Support)	
	Minimum	**Maximum**		**Minimum**	**Maximum**
1 - 10	$1,975.00	$7,575.00	$500.00	$1,475.00	$7,075.00
11 - 20	$1,975.00	$8,275.00	$725.00	$1,250.00	$7,550.00
21 - 50	$2,675.00	$9,675.00	$850.00	$1,825.00	$8,825.00
51 - 100	$2,675.00	$11,075.00	$1,350.00	$1,325.00	$9,725.00
101 - 200	$4,075.00	$15,275.00	$1,600.00	$2,475.00	$13,675.00

What is the Mode of Assessment for Cyber Trust Mark?

The mode of assessment (remote/onsite) will involve both review and verification of documents, as well as implementation and effectiveness.

What are the steps to obtaining CSA SG Cyber Safe Cyber Trust mark certification?



How is the cybersecurity preparedness tier being identified for organizations?

The organization can use the Cyber Trust mark risk assessment framework to identify which Cybersecurity Preparedness tier is more suitable for their needs.

The Cyber Trust mark risk assessment framework consists of a two-part self-assessment:

1. Risk Assessment of its cybersecurity profile
2. Cybersecurity Preparedness Assessment

The outcome of the self-assessment will provide the organization with an estimation of its cyber preparedness tier across the different domains, including a list of self-identified gaps against the applicable cyber preparedness domain statements. The organization should consider these gaps while assessing the residual risks for the various risk scenarios as part of the risk assessment. The organization shall also develop appropriate risk treatment plans and remediation activities based on their risk profile.

Which tier of Cybersecurity Preparedness does my organization belong to?

There are five Cybersecurity Preparedness tiers, with 10 to 22 domains under each tier. Enterprises can use the Cyber Trust mark risk assessment framework to identify which Cybersecurity Preparedness tier is more suitable for their needs.

CSA SG Cyber Safe Cyber Trust mark – Cybersecurity preparedness tiers

As the risk level of organizations vary, instead of prescribing specific cybersecurity measures, the Cyber Trust mark takes on a risk-based approach to guide organizations in identifying gaps in their implementation of the cybersecurity preparedness measures so that their implementation commensurate with their cybersecurity risk profile.

CYBER TRUST Advocate	Organizations with leading digital maturity level, large organizations or those operating in/providers to regulated sectors
CYBER TRUST Practitioner	Organizations with "starter" digital maturity level, medium and small organizations
CYBER TRUST Performer	Organizations with "performer" digital maturity level, large and some medium organizations
CYBER TRUST Supporter	Organizations with "starter" digital maturity level, small and some micro enterprises including "digital native" startups
CYBER TRUST Promoter	Organizations with "literate" digital maturity level, medium and some large organizations

	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

(Table by CSA)

Download the infographic on Cyber Essentials mark