

## 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.

#### Is there any Grant available for Cyber Trust Mark?

Yes, Enterprise Development Grant (EDG) for CSA Cyber Trust Certifications is available. Cyber Trust certifications are applied under the category - Market Access > Standards Adoption. The grant is only for eligible organizations. <https://www.csa.gov.sg/-/media/Csa/Documents/Programmes/SG-Cyber-Safe/Quick-Guide-EDG-Application-for-Cyber-Trust-certifications.pdf>

Inspiring trust for a more resilient world.

CSA SG Cyber Safe Cyber Trust mark – Pricing Table

CSA SG Cyber Safe Cyber Trust mark - Pricing Table

Number of Persons doing work under the organization's control	Low/Med/High Business Complexity/ Low/Med/High IT Complexity (Initial Year Fee)	
	Min	Max
1 to 100	12,200	24,800
101 to 200	13,600	28,300
201 to 300	15,700	31,800
301 to 500	18,500	37,400
501 to 1000	22,000	44,400
1001 to 1500	24,800	51,400
1501 to 2000	28,300	58,400
> 2000	Please consult BSI	

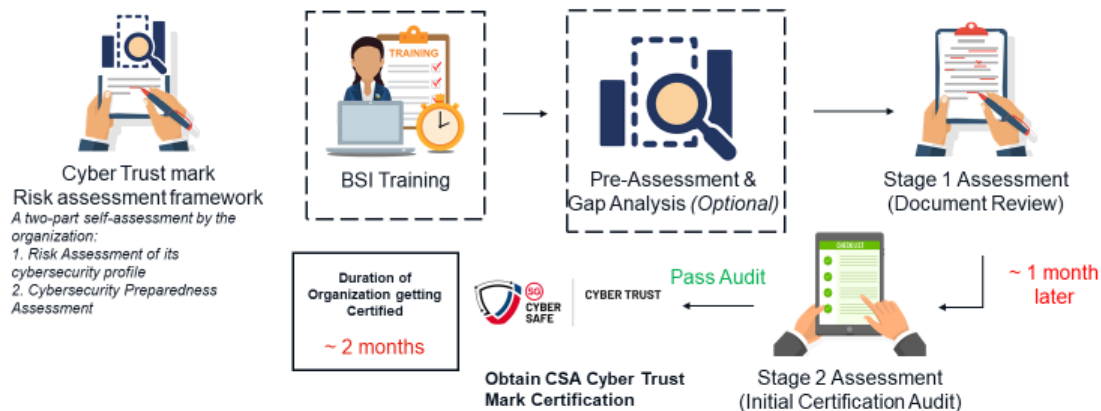
**Please note:** The fees indicated in Table are derived from the duration calculated considering the number of personnel under the organization's control and the impact factors considered based on the organization's business and IT complexity. These fees include audit fees (Stage 1 & 2), reporting and application fees. It excludes the annual audit year 2 and year 3 fees

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?

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



**How do I apply?**  
**For more information:** contact BSI Group Singapore Pte Ltd at [CSAinfo@bsigroup.com](mailto:CSAinfo@bsigroup.com) or call +65 6270 0777 / 9817 8586 / 9630 6425

**Frequently Asked Questions**

**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

**Frequently Asked Questions**

	<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>16 DOMAINS</b>	<b>19 DOMAINS</b>	<b>22 DOMAINS</b>

\*Measures in Cyber Essentials mark

(Table by CSA)

[Cybersecurity Certification for Enterprises – Cyber Trust mark \(csa.gov.sg\)](https://www.csa.gov.sg)

Inspiring trust for a more resilient world.