softScheck

— We Build Trust —

Contact Us

: enquiry@softscheck.sg

: softScheck APAC

: softScheck APAC

Cyber Trust Mark Advisory

Enterprise Development Grant (EDG) for CSA Cyber Trust Mark Certification is available!

Disclaimer Notes:

SOFTSCHECK shall exercise reasonable care to its best ability to guide the company towards development of a management system for successful certification; the company shall, however, assure SOFTSCHECK of its full cooperation and act in accordance with SOFTSCHECK' guidance and direction. The company shall otherwise be responsible for its own outcome – if it chooses its own course by deviating from SOFTSCHECK' advise. Successful certification can only be assured provided that the company acts strictly in accordance with SOFTSCHECK' advise throughout the project.

SOFTSCHECK reserves the copyrights of its methodology rendered and documents provided in the development / compilation / implementation of the system process. This includes copyrights of any written documents / articles provided by SOFTSCHECK in the course of the project. The company shall guarantee non-disclosure of such copyrights by either the company or its employees to any third-party, other than for the use for its project team members. Transfer of manual / procedures to other external parties or affiliates is a direct contravention to this agreement.

www.softscheck.sg

Fuelled by the pandemic, Singapore has experienced a ballooning number of cyber threats in recent years. Cyber-attacks continue to dominate news headlines with reported exposures of businesses to financial loss, loss of sensitive data, operational downtime, and negating business investments. Beyond these negative impacts, becoming victim to a cyber-attack tarnishes business reputation and affects customers' trust and confidence.

What is Cyber Trust Mark?

Cyber Trust Mark is a cybersecurity certification issued by The Cyber Security Agency of Singapore (CSA). This serves as a mark of distinction for businesses who put in place good cybersecurity practices and measures that matches their risk profile.

Which of Cyber Security Preparedness is your organization in?

There are five (5) cybersecurity preparedness tiers with 10 – 22 domains under each tier, as shown in the Figure below. Organizations can use the Cyber Trust Mark Risk Assessment framework to assess which tier is best suited to your 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		•	•	•	•
*Measures in Cyber Essentials mark	10 DOMAINS	13 DOMAINS	16 DOMAINS	19 DOMAINS	22 DOMAINS

Source: Cybersecurity Certification for Enterprises – Cyber Trust mark (csa.gov.sg)

Who is the Cyber Trust Mark for?

- Your business operations are robust and digitized
- You need to assess cybersecurity risks and preparedness
- You want to start implementing cybersecurity practices and international standards relating to IOT and cybersecurity such as ISO/IEC 27001 etc., but it seems daunting
- You are looking for a progressive pathway to adopt international information security standards (E.g., ISO/IEC 27001:2013)

Benefits of Cyber Trust Mark

- Increase business resilience
- Lower cyber risk and legal threat exposure
- Minimize risk of monetary penalties
- Earn trust and confidence from clients and partners
- Ensure a match of your cybersecurity risk and needs without over-investment

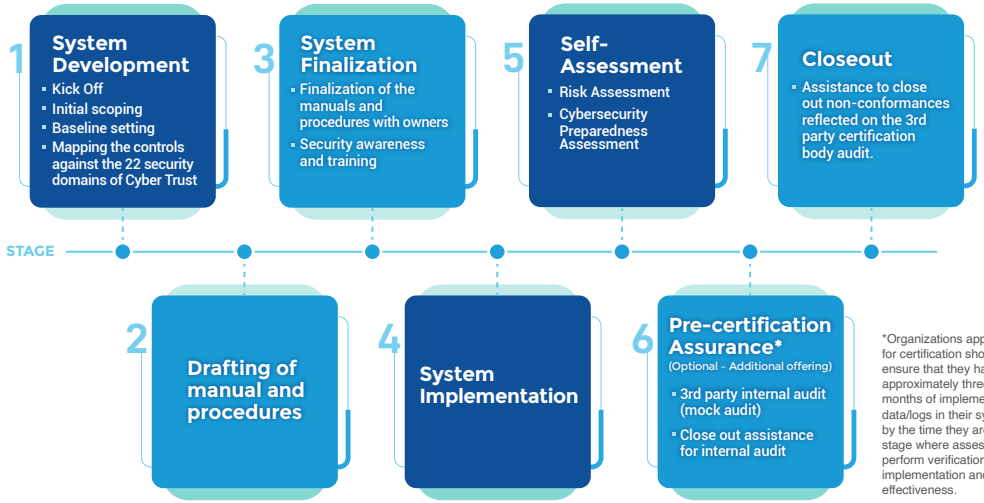
How can softScheck help you?

softScheck helps organizations achieve the Cyber Trust Mark in these ways:

- Provide expertise in areas of cybersecurity risk profile assessment
- Clear the path and provide a guided approach that saves time and hassle
- Support your organization through the arduous journey
- Substantially decrease the chances of failure

Approach and Methodology

We aim to handhold and walk with your organization throughout the various stages of your Cyber Trust Mark implementation and certification program. Our approach requires close engagement through the listed stages below:



*Organizations applying for certification should ensure that they have approximately three (3) months of implementation data/logs in their systems by the time they are at the stage where assessors perform verification of implementation and effectiveness.