SOCOTEC CERTIFICATION SINGAPORE PTE LTD

The power of foresight

SG Cyber Safe Programme

Since the COVID-19 pandemic, business dynamics have changed and more businesses go digital and there is a growing concern for enterprises to raise their cybersecurity posture. One of the program under this initiative by the Cyber Security Agency of Singapore (CSA) is Cyber Security Certification. The two certification marks are:

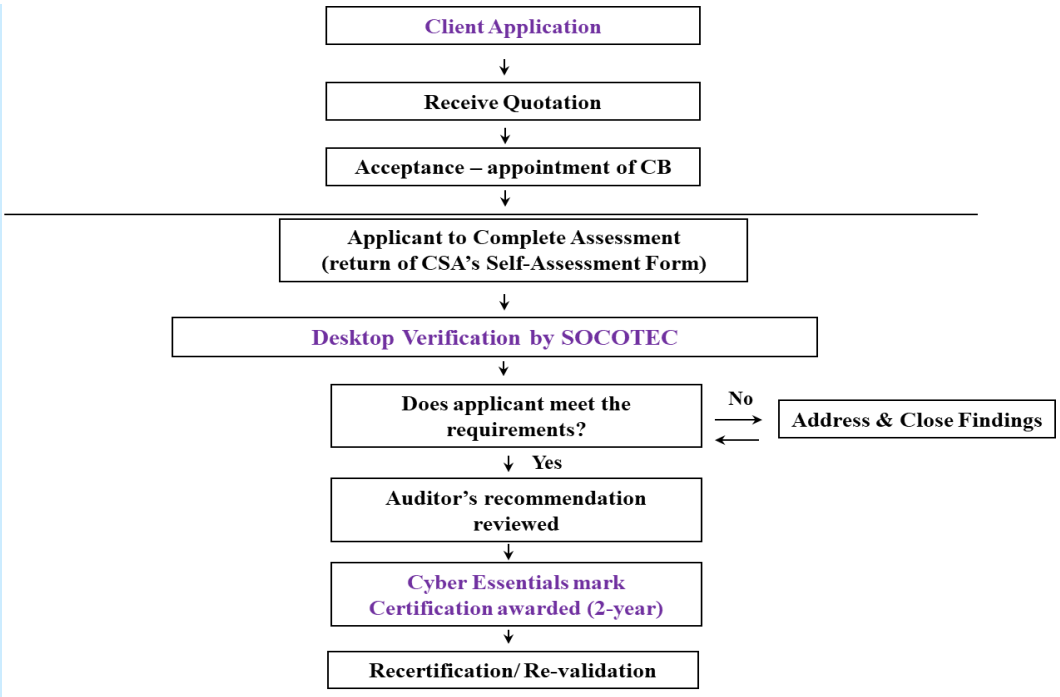
- **Cyber Essentials mark**
- **Cyber Trust mark**

Cyber Essentials mark

The Cyber Essentials mark is a cybersecurity certification for organisations that are embarking on their cybersecurity journey. It serves to recognize that the organization has put in place good cyber hygiene practices to protect their operations and their customers against common cyber attacks.

The Cyber Essentials mark is targeted at organisations with limited IT and/or cybersecurity expertise and resources to dedicate towards protecting IT assets and personnel. Cyber Essentials mark certification is valid for two (2) years, and to maintain the certification status, enterprises are required to undergo recertification/ revalidation assessment.

Overview of Assessment Process



Early Bird Incentive

**29Mar22-31Mar23*
**Only for 1st successful certification*

Profile of Enterprise	Fee Charged for Granting and Extending Certification	Maximum Level of Support from CSA (first successful application)	Certification Fee Charged to Industry (factoring in CSA's support)
Small SME (<10 employees)	**S$300**	S$100	S$200
Medium SME (10 – 99 employees)	**S$375**	S$200	S$175
Larger SME (100 – 200 employees)	**S$550**	S$250	S$300

For more information, please contact the following personnel:

- Ms. Chris Lim (chris@socotec.com)
- Ms. Salwa Halid (salwa.halid@socotec.com)

You may also visit: https://www.csa.gov.sg/Programmes/sgcybersafe/cybersecurity-certification-for-enterprises/cyber-essentials-mark

SOCOTEC CERTIFICATION SINGAPORE PTE LTD

The power of foresight

Cyber Trust mark

The Cyber Trust mark is a cybersecurity certification for organisations with more extensive digitalized business operations. It serves as a mark of distinction for the organization to prove that they have put in place good cybersecurity practices with their cybersecurity risk profile.

The Cyber Trust mark is targeted at larger or more digitalized organisations that have gone beyond cyber hygiene. These organisations may have higher risk levels and would correspondingly invest in expertise and resources to manage and protect their Information Technology (IT) infrastructure.

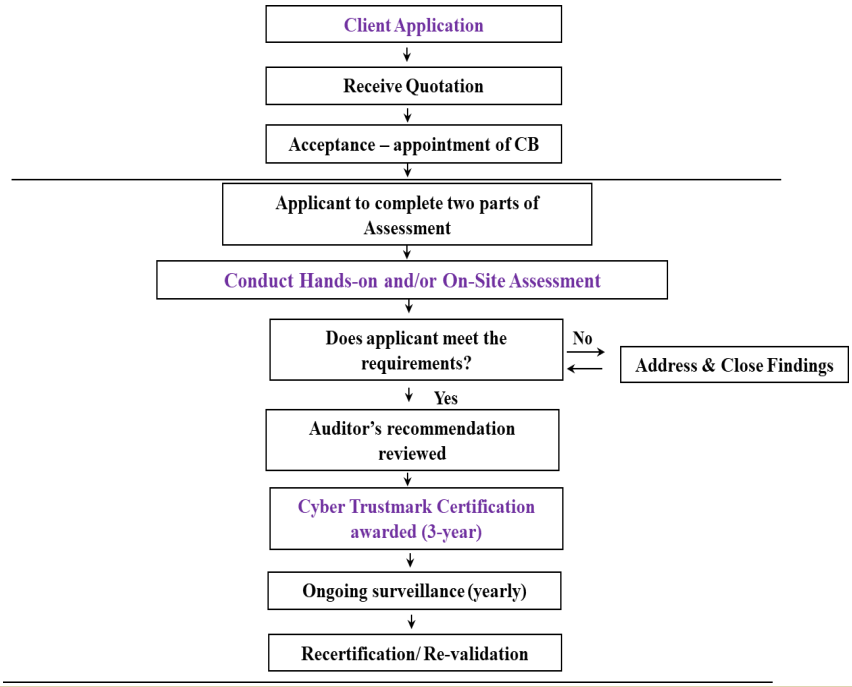
For Cyber Trustmark, the certification is valid for three (3) years, enterprises are required to undergo recertification/ revalidation assessment to continue the certification. On a yearly basis, enterprises under Cyber Trustmark will undergo interim technical audits and validation checks/ assessments.

There are five (5) cybersecurity preparedness tiers and progressively improve its system for higher recognition. The award of Trustmark from certification bodies are in accordance to the outcome of assessment where the entities fall under:

Indicative organization profile[1] (Digital maturity level[2], size, nature of industry/ business)	**Cybersecurity preparedness tiers**
Organisations with leading digital maturity level, large organisations or those operating in/providers to regulated sectors	**Advocate**
Organisations with "performer" digital maturity level, large and some medium organisations	**Performer**
Organisations with "literate" digital maturity level, medium and some large organisations	**Promoter**
Organisations with "starter" digital maturity level, medium and small organisations	**Practitioner**
Organisations with "starter" digital maturity level, small and some micro enterprises including "digital native" startups	**Supporter**

1 - This is a indicative reference only. In reality, organisations of the same size may have different risk profiles and correspondingly, need to be at different cybersecurity preparedness tiers as they may operate in different sectors, or their operations expose them to different nature of data and/ or cyber breach
2 - Description of digital maturity level aligns to terminology in IMDA Digital Acceleration Index (DAI)

Overview of Assessment Process



Start Your Journey with us...

Step 1: Discuss Your enquiry with us

Step 2: Submit Application & Ask for Quote

Step 3: Understand Certification Document and Perform Self-Assessment (refer to CSA self-assessment template)

Step 4: Implement & Prepare All Relevant Supporting Document

Step 5: Independent Assessment by Socotec

**Cyber Trust mark certification can be done concurrently with ISO 27001/ISO 27701/SS 584*

**Indicative Fees starts from S$1,100-S$1,650, fee will be reviewed after assessing the enterprise profile & scope of work applicable including the complexity of scope, no. of location(s) & cybersecurity preparedness levels.*

For more information, please contact:

- Ms. Chris Lim (chris@socotec.com)
- Ms. Salwa Halid (salwa.halid@socotec.com)

You may also visit: https://www.csa.gov.sg/Programmes/sgcybersafe/cybersecurity-certification-for-enterprises/cyber-essentials-mark