CYBER SAFE CERTIFICATION SCHEME

ATTAIN A MARK OF DISTINCTION FOR YOUR ORGANISATION'S ROBUST CYBER SECURITY POSTURE

The Cyber Safe Certification Scheme is an initiative launched by **Cyber Security Agency (CSA)**, which recognises organisations that have adopted and implemented good cyber security practices.

Revolving around **People, Processes and Technology,** the scheme takes on the risk-based approach with the aim to help identify and guide organisations to put in place adequate cyber security measures to protect and defend systems and operations against cyber-attacks.

At Privasec, we have a team of Governance, Risk and Compliance experts to guide and assist your organisation's compliance journey.

- ✓ **Tailored approach for lean compliance profile**
- ✓ **Detailed guidance from GRC experts to identify security gaps and uplift security posture**
- ✓ **Implementation of practical solutions and establishment of security roadmaps to address critical gaps and long terms solutions**
- ✓ **Presentation of the business case to demonstrate and explain the security investments to relevant stakeholders**

CYBER ESSENTIALS

Serves as a **mark of distinction** for organisations with **good cyber hygiene practices** to secure their operations and systems from common cyber-attacks.

- Catered for **Small and Medium Enterprises (SMEs)** – which often have limited IT and/or cybersecurity expertise and resources.
- Takes on a ***baseline control approach*** for protection against common cyber attacks that focuses on five aspects of Cyber Hygiene which include:
  - **Assets, Secure/Protect, Update, Backup, Respond**

2 Years Validity

Desktop assessment
(By an independent assessor)

CYBER TRUST

Serves as a **mark of distinction** for organisations with **comprehensive cybersecurity measures and practices** that are ***commensurable with their risk profile.***

- Catered for **larger or more digitalised organisations.**
- With extensive IT infrastructures, these organisations may have higher risk levels. Thus, investments in cyber security expertise and resources to manage and secure its IT infrastructure are paramount.
- Takes on a **risk-based approach,** to enable organisations to adopt and implement relevant cybersecurity practices that commensurate with their cyber risk profile.
- **Non-prescriptive,** applicability of controls depends on organisations' needs and risk profiles.
- **Five Cybersecurity Preparedness Tiers,** with 10-22 domains under each tier.
- **Integrated options to certify with ISO 27001 Standard**. (Depending on the organisation's readiness level)

3 Years Validity
(Annual surveillance)

- **Documentation**
- **Implementation and effectiveness**
  (By an independent assessor)

CYBER TRUST MARK - FIVE CYBERSECURITY PREPAREDNESS TIERS

INDICATIVE ORGANISATION[1] PROFILE (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	5 ADVOCATE
Organisations with "performer" digital maturity level, large and some medium organisations	4 PERFORMER
Organisations with "literate" digital maturity level, medium and some large organisations	3 PROMOTER
Organisations with "starter" digital maturity level, medium and small organisations	2 PRACTITIONER
Organisations with "starter" digital maturity level, small and some micro enterprises including "digital native" startups.	1 SUPPORTER

1 – Organisations of the same size may have different risk profiles, and correspondingly, need to be at different cybersecurity preparedness tiers
2 – Description of digital maturity level aligns to terminology in IMDA Digital Acceleration Index (DAI)

[Chart adapted from CSA]

Privasec
www.privasec.com

CONTACT US

+ 65 6610 9597
info@privasec.com