## 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)



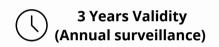






Serves as a mark of distinction for organisations with comprehensive cybersecurity measures and practices that are commensurable with their risk profile.

- 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 <u>10-22 domains under each tier.</u>
- Integrated options to certify with ISO 27001 Standard. (Depending on the organisation's readiness level)





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

## **CYBER TRUST MARK - FIVE CYBERSECURITY PREPAREDNESS TIERS** CYBERSECURITY INDICATIVE ORGANISATION¹ PROFILE **PREPAREDNESS TIERS** (Digital maturity level<sup>2</sup>, size, nature of industry/business) Organisations with leading digital maturity level, large **ADVOCATE** organisations or those operating in/providers to regulated sectors Organisations with "performer" digital maturity level, large and **PERFORMER** some medium organisations Organisations with "literate" digital maturity level, medium and **PROMOTER** Organisations with "starter" digital maturity level, medium and **PRACTITIONER** small organisations Organisations with "starter" digital maturity level, small and some **SUPPORTER** micro enterprises including "digital native" startups. 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]