

CSA Cyber Trust mark (SS 712)

Service information sheet. Cybersecurity, IT and Data Protection. Information checked 11 October 2026.

In brief

The CSA Cyber Trust mark (SS 712) certifies that an organisation manages cyber risk in proportion to its exposure. It uses five preparedness tiers and four pillars, is valid for three years with yearly audits, and is issued by CSA-appointed certification bodies. ICFC helps you choose the right tier, prepare, and train your team.

What it is

The Cyber Trust mark is CSA's risk-based cybersecurity certification for organisations with more extensive digital operations. The 2025 edition is published as Singapore Standard SS 712 and now covers classical IT, cloud, operational technology (OT) and AI security.

Who it is for

Organisations that handle sensitive data, serve enterprise or government buyers, or rely heavily on digital systems, cloud or OT.

Tiers

Five cybersecurity preparedness tiers: Supporter, Practitioner, Promoter, Performer and Advocate. CSA's risk assessment framework points each organisation to its tier, and each tier carries between 10 and 22 preparedness domains. The tier reflects how much cyber risk the business carries, not its size.

Pillars

Classical cybersecurity is the base pillar. Cloud security, operational technology (OT) security and AI security are added as pillars where they apply to your operations.

CSA funding (Cyber Trust 2025)

For the classical pillar, CSA's maximum support ranges from S\$1,375 (1 to 10 end-points) to S\$2,250 (101 to 200 end-points). Each added cloud, OT or AI pillar attracts S\$225, or S\$450 for 101 to 200 end-points, giving up to S\$3,600 in total. First certification only, for Singapore-incorporated SMEs and non-profits, until 6 February 2028. Figures from CSA, checked 11 October 2026.

How ICFC helps

Service	What we offer
Audit	Third-party assessments: Certification is awarded under the scheme run by the Cyber Security Agency of Singapore (CSA). Where appointed, our auditors carry out assessments on behalf of the certification body; the certificate or mark is never issued by ICFC. Second-party audits: Supplier and partner checks against the scheme requirements, on behalf of your organisation. Readiness and internal audits: A pre-assessment that shows exactly what the formal assessment will look for, with a prioritised action list.
Consulting	Funding: CSA's certification funding is deducted by the certification body from its own fee. Our consultancy is quoted separately and is not covered by that funding. Non-grant: A fixed-scope engagement: gap assessment, documentation, implementation coaching, internal audit and management review, and support through the formal audit or assessment. How we work: Practical, proportionate systems that your staff can run after we leave.
Training	Classroom: Public and in-house classroom courses on SS 712: awareness, implementation and internal auditor levels. Online LMS: Self-paced and live-online courses on the ICFC Digital LMS, with progress tracking and certificates of completion. Funding: Funding depends on each course's approval status, shown on the course page in the LMS.

Funding

CSA certification funding. This mark is funded by CSA rather than EDGE. CSA funds the first successful certification only, for SMEs and non-profit organisations incorporated in Singapore, until 6 February 2028. The amount is deducted from the fee charged by the CSA-appointed certification body. Consultancy fees are not covered by this funding.

Impartiality

Impartiality comes first. Every engagement begins with a conflict-of-interest check. We keep consulting and auditing roles separate, and our auditors never audit, on behalf of a certification body, an organisation that ICFC has consulted on the same scope within the period set by that body.

Frequently asked questions

Q. Which Cyber Trust tier do we need?

A. Your tier comes from CSA's risk assessment template. We run it with you, explain the result, and plan the controls for that tier only, so you do not over-build.

Q. Is Cyber Trust the same as ISO/IEC 27001?

A. No. Both are risk-based, and CSA publishes a mapping between them, but they are separate certifications. Organisations certified to one can reuse much of the evidence for the other.

Q. How long is the certificate valid?

A. Three years, with an audit each year to keep it active.

Q. Can we start with Cyber Essentials instead?

A. Yes. Cyber Essentials suits organisations at the start of their journey and is a natural stepping stone to Cyber Trust.

Related services

- CSA Cyber Essentials mark
- ISO/IEC 27001 Information Security Management System (ISMS)
- ISO/IEC 27701 Privacy Information Management System (PIMS)
- ISO/IEC 42001 Artificial Intelligence Management System (AIMS)

Talk to us

Phone, WhatsApp, Telegram and WeChat: +65 8601 7001. Email: admin@icfc.com.sg. Web: icfc.com.sg.
Learning platform: icfc.digital.

This sheet is a summary for general information. Scheme owners, accreditation bodies and funding agencies decide requirements, certification and eligibility; please confirm on their official websites. ICFC does not issue certificates, attestation reports or maturity ratings, and does not give legal advice. ICFC Pte Ltd, UEN 201402439E.