

ISO/IEC 27001 Information Security Management System (ISMS)

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

In brief

ISO/IEC 27001 is the international standard for information security management systems (ISMS). It helps organisations identify and treat information security risks through a managed set of controls. Certification is by accredited bodies, and Enterprise Singapore lists it under EDGE with up to 50% support for SMEs and 30% for non-SMEs.

What it is

ISO/IEC 27001 sets requirements for an information security management system, including the assessment and treatment of information security risks. It applies to organisations of every type, size and sector. The current edition is ISO/IEC 27001:2022.

Who it is for

Organisations that hold client, financial or sensitive data, serve enterprise or overseas buyers, or want one recognised framework for information security across the business.

Links to Singapore schemes

CSA publishes a mapping between the Cyber Trust mark (2025) and ISO/IEC 27001:2022, so evidence can be reused. ISO/IEC 27001 also forms the base for cloud and privacy extensions such as ISO/IEC 27017, 27018 and 27701.

How ICFC helps

Service	What we offer
Audit	Third-party audits: Third-party certification audits for ISO/IEC 27001 are delivered by our auditors on behalf of accredited certification bodies. The certificate is issued by the certification body, not by ICFC. Second-party audits: Supplier and partner audits against ISO/IEC 27001 on behalf of your organisation, with clear findings you can act on. Internal audits: First-party internal audits of your information security management by experienced auditors, combinable with other standards in one integrated audit.
Consulting	Grant-supported (EDGE): ICFC's consultancy is led by consultants certified to SS 680:2021, which Enterprise Singapore requires for consultancy support under EDGE Standards activities. The certification is held by our individual consultants, not by ICFC as a company. Our proposal names the certified consultant who will lead your project and includes the SS 680 certification details, quotation and scope that EDGE asks for. You apply on the Business Grants Portal before any work starts or any payment is made. Vendors cannot apply, pay or claim for you, the consultant named in the Letter of Offer must bill the claim invoices, and vendors cannot be changed after approval. Support is subject to Enterprise Singapore's assessment and approval. For our SS 680 certified consultants' roles, certificate numbers, issuing body and expiry dates, or a link to the issuing body's register, please email us through the contact form. 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 ISO/IEC 27001: 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

Listed under EDGE Standards (confirmed). Enterprise Singapore lists this standard under the EDGE Grant. Support is up to 50% for SMEs and up to 30% for non-SMEs, covering professional services and first-year certification by an accredited body. It counts toward the shared S\$100,000 annual EDGE cap.

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. Is ISO/IEC 27001 eligible for EDGE?

A. Yes. Enterprise Singapore lists ISO/IEC 27001 under EDGE Digitalisation Standards with up to 50% support for SMEs and 30% for non-SMEs, subject to eligibility.

Q. Should we choose ISO/IEC 27001 or Cyber Trust?

A. Cyber Trust is Singapore's risk-tiered mark; ISO/IEC 27001 is recognised internationally. Many organisations hold both, using CSA's mapping to avoid duplicate work.

Q. What is the Statement of Applicability?

A. A document that lists the Annex A controls, whether each applies to you, and why. Auditors review it closely.

Q. Can it be audited together with other standards?

A. Yes. Our auditors routinely combine information security, privacy, cloud and quality standards in one integrated audit.

Related services

- CSA Cyber Trust mark (SS 712)
- ISO/IEC 27701 Privacy Information Management System (PIMS)
- ISO/IEC 27017 Information security controls for cloud services
- 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.