

ISO 27001

ISO 27001 is the international standard for managing information security. This is what it covers, how certification works and why Swedish organisations increasingly need it.

WHAT IT IS

ISO 27001 is the international standard for an information security management system, or ISMS. It sets out how an organisation identifies its information risks and puts controls in place to manage them. It is not only an IT concern. It is a business standard that gives customers, regulators and boards independent proof that security is being managed.

WHY IT MATTERS

96,709

Valid ISO/IEC 27001 certificates worldwide.

ISO Survey 2024

93

Annex A controls in ISO/IEC 27001:2022, grouped into four themes.

ISO/IEC 27001:2022

~200 of 290

Swedish municipalities and regions affected when one HR-software supplier was breached in 2025.

The Record, 2025

WHAT HAPPENED

In August 2025 attackers hit Miljödata, a supplier of HR and sick-leave software used by most Swedish municipalities. The breach disrupted services for around 200 of Sweden's 290 municipalities and regions, and data on about 1.5 million people was later published on the dark web. It shows how one supplier's security can become your problem. (The Record, 2025)

MYTHS AND FACTS

MYTH

ISO 27001 is an IT project.

FACT

It is a management-system standard owned by leadership. It covers people and process, not only technology.

MYTH

A certificate means you cannot be breached.

FACT

Certification proves you manage risk to a recognised standard. Certified organisations have still been breached, so it lowers risk rather than removing it.

MYTH

You must implement all 93 Annex A controls.

FACT

You apply the controls your risk assessment justifies and record the rest in your Statement of Applicability. Annex A is a reference set.

THE LEGAL DUTY

ISO 27001 is not required by law, but it helps you meet duties that are. NIS2, in force in Sweden as Cybersäkerhetslagen since 15 January 2026, requires the risk-management measures in Article 21 and makes the management body accountable under Article 20. An ISO 27001 system gives boards much of the evidence both demand.

GET HELP

eBuilder Security provides Sweden-based cybersecurity advisory that helps organisations scope, build and certify an ISO 27001 management system. Read the full guide at the link below.

[Read the Full Article →](#)