ISO/IEC 27014

< Previous standard ^ Up a level ^ Next standard >

ISO/IEC 27000
ISO/IEC 27001
ISO/IEC 27002
ISO/IEC 27003
ISO/IEC 27004
ISO/IEC 27005
ISO/IEC 27006
ISO/IEC 27007
ISO/IEC TS 27008
ISO/IEC 27010
ISO/IEC 27011
ISO/IEC 27013
ISO/IEC 27014
ISO/IEC TR 27016
ISO/IEC 27017
ISO/IEC 27018
ISO/IEC 27019
ISO/IEC 27021
ISO/IEC TS 27022
ISO/IEC TR 27024
ISO/IEC TS 27028
ISO/IEC TR 27029
ISO/IEC 27031
ISO/IEC 27032
ISO/IEC 27033
ISO/IEC 27034
ISO/IEC 27035

ISO/IEC 27014:2020 / ITU-T X.1054 — Information security, cybersecurity and privacy protection — **Governance of information security** *(second edition)*

Abstract

"[ISO/IEC 27014] provides guidance on concepts, objectives and processes for the governance of information security, by which organisations can evaluate, direct, monitor and communicate the information security-related processes within the organisation. The intended audience for [ISO/IEC 27014] is: governing body and top management; those who are responsible for evaluating, directing and monitoring an information security management system (ISMS) based on ISO/IEC 27001; those responsible for information security management that takes place outside the scope of an ISMS based on ISO/IEC 27001, but within the scope of governance. [ISO/IEC 27014] is applicable to all types and sizes of organisations. All references to an ISMS in [ISO/IEC 27014] apply to an ISMS based on ISO/IEC 27001. [ISO/IEC 27014] focuses on the three types of ISMS organisations given in Annex B. However, [ISO/IEC 27014] can also be used by other types of organisations."

[Source: ISO/IEC 27014:2020/ITU-T X.1054]

Introduction

This standard, produced by ISO/IEC JTC 1/SC 27 in collaboration with the **I**nternational **T**elecommunications **U**nion's **T**elecommunication Standardization Sector (ITU-T), is specifically aimed at helping organisations **govern their information security arrangements**.

Scope and purpose

The standard "provides guidance on concepts, objectives and processes for the governance of information

ISO/IEC 27036
ISO/IEC 27037
ISO/IEC 27038
ISO/IEC 27039
ISO/IEC 27040
ISO/IEC 27041
ISO/IEC 27042
ISO/IEC 27043
ISO/IEC 27045
ISO/IEC 27046
ISO/IEC 27050
ISO/IEC 27070
ISO/IEC 27071
ISO/IEC 27090
ISO/IEC 27091
ISO/IEC 27099
ISO/IEC TS 27100
ISO/IEC 27102
ISO/IEC TR 27103
ISO/IEC TR 27109
ISO/IEC TS 27110
ISO/IEC TS 27115
ISO/IEC 27116
ISO/IEC 27400
ISO/IEC 27402
ISO/IEC 27403
ISO/IEC 27404
ISO/IEC TR 27550
ISO/IEC 27551
ISO/IEC 27553
ISO/IEC 27554
ISO/IEC 27555
ISO/IEC 27556
ISO/IEC 27557
ISO/IEC 27559
ISO/IEC TS 27560

security, by which organisations can evaluate, direct, monitor and communicate the information security-related processes within the organisation."

In a nutshell, **through sound governance arrangements, information security management achieves business objectives** - a very important and powerful concept.

As with other ISO27k standards, it is "applicable to all types and sizes of organisations", particularly those with one or more ISO 27001-style ISMSs encompassing either the entirety or certain parts of the organisation, or where a single ISMS applies across several businesses or business units (*e.g.* within a group structure).

Structure and content

After the conventional introductory sections, the three main clauses are:

6. Governance and management standards;
7. Entity governance and information security governance;
8. The governing body's requirements on the ISMS;

... followed by three informative annexes:

A. Governance relationship;
B. Types of ISMS organization;
C. Examples of communication.

The standard explains four "processes" (key aspects of governance):

1. **Evaluation:** senior management considers proposals and plans for information security management (*e.g.* "We will adopt an ISO27001 ISMS");
2. **Direction:** preparing strategies, policies and objectives for *information security* that align with and support the achievement of the organisation's *business* objectives (*e.g.* "It is imperative that we both protect and exploit valuable information");
3. **Monitoring** the performance of information security through management information flows and internal reporting arrangements (*e.g.* "We track the following security metrics: ...");
4. **Communication:** ensures that all those within the organisation who are actively involved in directing, overseeing, driving, guiding and monitoring information security are 'singing from the same hymn sheet', while external stakeholders (such as its owners and regulatory authorities) are assured that information risk is being competently managed.

It also lays out six information security objectives that the governance and management arrangements should satisfy:

1. **Establish integrated comprehensive entity-wide information security** since the information at risk is found and used (legitimately exploited), and hence deserves protection, throughout the organisation;
2. **Make decisions using a risk-based approach** - fundamental to all the ISO27k standards and at all levels of the ISMS from governance and strategy through management to routine operations (e.g. risk-assessing identified incidents to determine the priority and nature of the responses required);
3. **Set the direction of acquisition** - as in corporate mergers and acquisitions, as opposed to procuring goods and services;
4. **Ensure conformance with internal and external requirements** through assurance such as auditing of information security activities;
5. **Foster a security-positive culture** - an excellent suggestion, albeit easier said than done;
6. **Ensure the security performance meets current and future requirements of the entity** - there is a need for suitable management oversight, monitoring and measurement (metrics) in relation to *current* requirements, of course, but what about the *future*? Food for thought here.

Status of the standard

The *first* edition was published in **2013**, dual-numbered as ISO/IEC 27014 and ITU-T recommendation X.1054 with identical text.

The *second* edition was published by ISO/IEC in **2020** and then released by ITU-T as a **free** PDF download in 2021. As of this writing, a printed version is available for US$31 from Amazon.

Personal comments

ISO/IEC 27561
ISO/IEC 27562
ISO/IEC TR 27563
ISO/IEC 27564
ISO/IEC 27565
ISO/IEC 27566
ISO/IEC 27568
ISO/IEC 27569
ISO/IEC TS 27570
ISO/IEC 27573
ISO/IEC 27701
ISO/IEC 27706
ISO 27799

ISO/IEC 27014 refers to '**information risk management**' - a minor but important distinction from the usual terms 'information security risk' and 'information security management'. Security (as in controls to reduce/mitigate risk) is not the only way to treat risks to information: they can also be avoided, shared and accepted. Personally, I wish the remaining ISO27k standards would adopt 'information risk' (defined along the lines of "risk pertaining to information") in place of 'information security risk' (a term that is not actually defined as such) but, so far, SC 27 management has blocked the move and we have not had the opportunity to debate it. I am merely a lone and tired kayaker nudging ISO's supertanker.

In the course of drafting the second edition, SC 27 discussed the application of principles from ISO 38500 ("Corporate governance of IT") to information security, and considered the relationship between information security governance and other governance and management disciplines. ISO/IEC 27014 refers to governance for information security as an integral part of the organisation's corporate governance with strong links to IT governance, but is arguably a bit vague on the details.

The definition of 'governing body' obliquely notes that, along with 'executive management', both are parts of 'top management' which ISO/IEC 27000 defines as "the person or group of people who directs and controls an organisation at the highest level". In essence, the standard hints that senior management has distinct or separable governance (strategic direction-setting) *and* hands-on executive management roles.

The summary points out that the standard "provides the mandate essential for driving information security initiatives throughout the organisation." At present, this is typically achieved in part by senior management mandating an overarching organisation-wide information security policy that is supported and amplified by lower level security policies, standards, procedures, guidelines and other security awareness materials. The standard does not go into depth on other related aspects such as the information security, risk and compliance management structures, reporting lines, divisions of responsibility, delegated authorities and so forth, largely I guess because of the differences between organisations.

As an information security professional with a keen interest in security awareness, I am gratified to note that, in order to "establish a positive information security culture, the governing body should require, promote and support coordination of stakeholder activities to achieve a coherent direction for information security. This will support the delivery of security education, training and awareness programs." 'A coherent direction' indeed. Nice idea. I approve.

ISO 37000:2021 "Guidance for the governance of organisations" could be the basis for updating ISO/IEC 27014 to utilise common concepts and terms. Maybe. At some point.

< Previous standard ^ Up a level ^ Next standard >