ISO/IEC 27000:2018 — Information technology — Security techniques — **Information security management systems — Overview and vocabulary** *(fifth edition)*

Abstract

Summary podcast

"ISO/IEC 27000:2018 provides the overview of information security management systems (ISMS). It also provides terms and definitions commonly used in the ISMS family of standards. [ISO/IEC 27000] is applicable to all types and sizes of organization (e.g. commercial enterprises, government agencies, not-for-profit organizations). The terms and definitions provided in [ISO/IEC 27000]: cover commonly used terms and definitions in the ISMS family of standards; do not cover all terms and definitions applied within the ISMS family of standards; and do not limit the ISMS family of standards in defining new terms for use."

[Source: ISO/IEC 27000:2018]

Introduction and scope

ISO/IEC 27000 gives an overview of information security management systems (and hence the ISO27k standards), and a glossary that formally and explicitly defines many (but not all) of the specialist terms as they are used within the standards.

ISMS/ISO27k vocabulary section

The vocabulary or glossary of carefully-worded **formal definitions** covers many of the specialist information security-related terms used in the ISO27k standards. Information security, like most technical subjects, uses a complex web of terminology that continues to evolve. Several core terms in information security (such as "risk" and "cyber") have different meanings or interpretations according to the context, the author's intention and the reader's preconceptions. Few authors take the trouble to define precisely what they mean but such ambiguity is distinctly unhelpful in the standards arena as it leads to confusion. Apart from anything else, it would be awkward to assess and certify conformity with ISO/IEC 27001 if the specialist terms meant different things to the assessors and the assessed!

The vocabulary in ISO/IEC 27000 is applicable throughout the global information security profession although some individuals and groups differ, sometimes with good reason, creating occasional misunderstandings, clashes, and conceptual chasms. Even if you happen to disagree with the definitions here, it is worth becoming familiar with them as some of your professional contacts will implicitly expect the ISO/IEC versions.

ISO/IEC 27000 largely supersedes **ISO/IEC Guide 2**:1996 "Standardization and related activities – General vocabulary", **ISO Guide 73**:2009 "Risk management – Vocabulary – Guidelines for use in standards", and **ISO/IEC 2382-8**: "Information technology - Vocabulary Part 8: Security". It also includes definitions taken from a few non-ISO27k ISO standards. Terms that are reproduced unchanged from other ISO standards such as **ISO 9000**

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

are not always entirely appropriate as such in the information security context. They are not necessarily used in the ISO27k standards in full accordance with the original definitions or intended meanings. However, as the definitions are gradually updated or superseded, the lexicon is evolving into a *reasonably* coherent and consistent state across the whole ISO27k suite - a remarkable achievement in its own right given the practical difficulties of coordinating the effort across a loose collection of separate committees, editing projects, editors and managers, developing the language and concepts as we go.

ISMS/ISO27k overview section

The **overview** of **I**nformation **S**ecurity **M**anagement **S**ystems introduces information security, risk and security management, and management systems. It is a reasonably clear if rather wordy description of the ISO27k approach and standards, from the perspective of the committee that wrote them. There is only one diagram, unfortunately, and all that does is group similar types of ISO27k standards together, but, hey, that leaves room for supplementary guidance ... such as this website!

Status of the standard

The *first* edition was published in **2009**.

It was updated in **2012**, **2014**, **2016** and **2018**.

The current 2018 *fifth* edition is available legitimately from ISO for **free**. This was a minor revision of the 2016 *fourth* edition with a section on abbreviations, and a rationalisation of the metrics-related definitions following the 2016 rewrite of ISO/IEC 27004.

The *sixth* edition of ISO/IEC 27000 is a work-in-progress. In accordance with ISO directives, the current edition's vocabulary will be moved to an annex containing a "definition and explanation of commonly used terms in the ISO/IEC 27000 family of standards" - more specifically, the glossary will apply to ISO27k standards belonging to ISO/IEC JTC 1/SC 27/WG 1 (ISO/IEC 27001 to ISO/IEC 27011, ISO/IEC 27013, ISO/IEC 27014, ISO/IEC 27016, ISO/IEC 27017, ISO/IEC 27019, ISO/IEC 27021 to ISO/IEC 27024, ISO/IEC 27028 and ISO/IEC 27029). Terms will be grouped conceptually in the annex rather than alphabetically. However, various specialist terms used in ISO/IEC 27000 itself are to be defined in clause 3 as usual.

The new *sixth* edition will be a lot shorter, halving the pages count.

Publication of the *sixth* edition is due by 2026, possibly later this year.

It is at **D**raft **I**nternational **S**tandard stage and has been submitted to ISO secretariat for processing. The title is to become "*Information security, cybersecurity and privacy protection — Information security management systems — Overview*".

Personal comments

A new clause 4 "Concepts and principles" in the *sixth* edition is intended to clarify the fundamentals underpinning information risk and security management.

The information security controls in ISO/IEC 27001 Annex A, '27002, '27010, '27011, '27017 and '27019 are to be termed "Candidate necessary information security controls" - a curious and ambiguous turn of phrase reflecting the committee's persistent difference of opinion in this area. 'Necessary' is for the organisation to determine according to its evaluation of information risks relative to its risk appetite. 'Candidate' is clearly *not* 'required' and is less than 'suggested', but still some readers (and poorly-trained auditors) may feel the controls are to be implemented by default.

Given the chance, I would replace "information security risk" *throughout* the ISO27k standards with the shorter, simpler and more appropriate term "information risk". "Information security risk" is not formally defined as a complete phrase and doesn't even make sense: it is presumably trying to indicate that we are talking about risk in the context of information security, but it could be interpreted as "risk *to* information security" which I guess would including things such as failing to identify novel risks, and lack of management support for the function: those are risks, but they are not the focus of ISO27k.

"Information risk", in contrast, is reasonably self-evident but, if the committee feels the desperate need for an explicit definition, I suggest something as simple as "risk relating to or involving information" or even "risk pertaining to information", where both risk and information are adequately defined in dictionaries (whereas the current ISO27k definition of risk is unhelpful).

Thus far, I have failed to persuade the committee to accept this terminological change, which admittedly would ripple through most of the ISO27k standards. However, clause 4.1.2 is expected to include the following concerning information:

> *"Information is an asset that, like other important business assets, is essential to an organization's business and, consequently, needs to be suitably protected."*

OK, yes it deserves adequate protection, but it *also* deserves legitimate exploitation for business purposes. That duality is something that management should address systematically using the ISMS as a framework.

> *"It does not matter whether the information is owned by the organization or is entrusted to its care by*

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

> *a third party, e.g., a customer."*

Patently ownership of information *does* matter, so that statement is plain wrong. Protection and exploitation of information matter to the owners of both business/commercial/proprietary and personal information (including that belonging to employees, by the way). Even public-domain information can be of value to society, groups or individuals, while inaccurate, outdated, incomplete, misleading, coercive, manipulative or malicious information is of concern regardless of who owns it.

I suspect that second sentence was specially supposed to build upon the first but somehow the linkage has been lost in translation, with unintended consequences.

Pressing ahead:

> *"Information can be stored in many forms, including digital form (e.g. data files stored on electronic or optical media), material form (e.g. on paper), as well as information in the form of knowledge. Information can be transmitted by various means including courier, electronic or verbal communication. Whatever form information takes, or how it is transmitted, it always needs appropriate protection."*

All good so far, but then ...

> *"In many organizations, information is dependent on information and communications technology. This technology is often an essential element in the organization and assists in facilitating the creation, processing, storing, transmitting, protection and destruction of information."*

The final paragraph reveals the longstanding systemic bias towards *technology* (in particular, IT) throughout the ISO27k standards. While clearly it is true that information security controls based on technology (information, operational, communications, smart *and* virtual technologies in fact) play a large part in protecting digital data, technology alone will never completely replace the need for humans to protect information as well, including the use of physical and organisational controls (such as policies, contracts and assurance measures),. And last but not least, the controls are specified, designed, used and managed by humans, while security incidents affect humans. In short, it's humans all the way.

^ Up a level ^ Next standard >