ISO/IEC 27010

ISO/IEC 27010:2015 — Information technology — Security techniques — **Information security management for inter-sector and inter-organisational communications** *(second edition)*

Abstract

"ISO/IEC 27010:2015 provides guidelines in addition to the guidance given in the ISO/IEC 27000 family of standards for implementing information security management within information sharing communities. This International Standard provides controls and guidance specifically relating to initiating, implementing, maintaining, and improving information security in inter-organisational and inter-sector communications. It provides guidelines and general principles on how the specified requirements can be met using established messaging and other technical methods. This International Standard is applicable to all forms of exchange and sharing of sensitive information, both public and private, nationally and internationally, within the same industry or market sector or between sectors. In particular, it may be applicable to information exchanges and sharing relating to the provision, maintenance and protection of an organisation's or nation state's critical infrastructure. It is designed to support the creation of trust when exchanging and sharing sensitive information, thereby encouraging the international growth of information sharing communities."

[Source: ISO/IEC 27010:2015]

Introduction

This standard provides guidance on sharing information about information risks, security controls, issues and/or incidents between industry sectors and/or nations, particularly those affecting "critical infrastructure".

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

Scope

ISO/IEC 27010 provides guidance on information security interworking and communications between industries in the same sectors, in different industry sectors and with governments. It applies both in times of crisis affecting critical infrastructure and under normal business circumstances to meet legal, regulatory and contractual obligations.

Purpose and justification

Sometimes it is necessary to share confidential information regarding information-related threats, vulnerabilities and/or incidents between or within a community of organisations. For example, when private companies, governments, law enforcement and CERTs collaborate on the investigation, assessment and resolution of serious pan-organisational and often international cyberattacks.

Such information is often highly sensitive and it typically needs to be restricted to certain individuals within the recipient organisations. Information sources may need to be kept anonymous. Such information exchanges typically happen in a highly charged and stressful atmosphere under intense time pressures - hardly the most conducive environment for establishing trusted working relationships and agreeing on suitable information security controls. The standard should help by laying out common ground-rules for security.

The standard provides guidance on methods, models, processes, policies, controls, protocols and other mechanisms for the sharing of information securely with trusted counterparties on the understanding that important information security principles will be respected.

Status of the standard

The *first* edition was published in **2012**.

The current *second* edition was published in **2015**. It was confirmed by SC 27 without change in 2021.

Personal comments

While the actual information risks arising from the sharing of information concerning information security incidents *etc*. between disparate organisations will of course depend on the specifics of the particular situation at hand (*e.g.* the nature of the incidents, the protagonists, the victims and the organisations involved), the following *generic* list of potential information risks and security issues in this area exemplifies the broad range of matters that may need to be taken into account in practice:

- Addressing information security aspects of the process (*e.g*. writing and implementing policies and procedures along with training and awareness activities for those involved in the process, and conceivably independent assessment or audits to confirm that the arrangements conform to ISO/IEC 27010 and/or other applicable ISO27k standards such as ISO/IEC 27001, ISO/IEC 27002 and ISO/IEC 27005);
- Disclosing initial information and knowledge about the situation at hand prior to formalizing the arrangements, in order to prompt the recipient/s to consider their role and for disclosing parties to consider the risks involved in disclosing further information;
- Building trusted relationships between the organisations directly concerned, communicating and collaborating;
- Trust relationships with other organisations that may also be involved (*e.g*. if communications are routed through some sort of agency) or are somehow drawn-in to the situation, including business partners and those that may have to be informed or engaged in the process as a statutory or other duty;
- Determining and declaring or defining specific information security requirements (implies some form of information risk analysis by the disclosing parties for sure, and perhaps by the receiving parties);
- Communicating information risks and security control requirements, obligations, expectations or liabilities unambiguously (*e.g*. using a mutually-understood lexicon of terms based on ISO27k, and comparable information classifications);
- Assessing and accepting security risks and obligations (*e.g*. in some form of contract or agreement, whose existence and contents may also be confidential);
- Communicating information securely (*e.g.* using suitable cryptographic controls), preventing it from being sent to the wrong counterparties, intercepted, deleted, spoofed, duplicated, repudiated, damaged, modified or otherwise called into doubt deliberately by some third party or through inadequate controls and errors;
- Version controls and appropriate authorization for both disclosure and acceptance of valuable information;
- Risks and controls relating to the collection, analysis, ownership, protection and onward disclosure of information regarding the situation at hand by the recipient parties engaged in an investigation (*e.g.* limitations on using the information for purposes not directly associated with the incident at hand);

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

- Adequately protecting the information and perhaps others assets entrusted to the recipient organisations and individuals;
- Compliance and where appropriate enforcement activities such as imposition of penalties *etc*. if promises are broken, trust is misplaced or accidents happen;
- Unacceptable delays or other constraints on the communication of important information due to the risk assessment, security and related activities;
- The possible effects on collection, handling, storage, analysis and presentation of forensic evidence;
- Any limitations on post-incident disclosures such as incident management reporting, public press-releases, legal action *etc*.;
- Systematic process improvement, leading to greater mutual trust and stronger security arrangements for future situations.

The published standard doesn't cover these aspects explicitly, unfortunately. I feel it would have been more comprehensive and valuable if it had.

< Previous standard ^ Up a level ^ Next standard >