TECHNICAL REPORT

ISO/IEC TR 27103

First edition
2018-02

Information technology — Security techniques — Cybersecurity and ISO and IEC Standards

Technologies de l'information — Techniques de sécurité — Cybersécurité et normes ISO et IEC

Reference number
ISO/IEC TR 27103:2018(E)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva, Switzerland
Tel. +41 22 749 01 11
Fax +41 22 749 09 47
copyright@iso.org
www.iso.org

Published in Switzerland

Contents

Page

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular the different approval criteria needed for the different types of ISO documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation on the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see the following URL: www.iso.org/iso/foreword.html.

This document was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

Introduction

Security on the Internet and other networks is a subject of growing concern. Organizations around the world, in both government and industry sectors, are seeking ways to address and manage cybersecurity risks, including via baseline cybersecurity measures that can be implemented as requirements or guidance. The demonstrated security and economic value of utilising existing best practices to develop approaches to cyber risk management has led organizations to assess how to use and improve upon existing approaches.

Perspectives, and consequent approaches, to risk management are affected by the terminology used, e.g. “cybersecurity” versus “information security”. Where similar risks are addressed, this different perspective can result in “cybersecurity” approaches focusing on external threats and the need to use information for organizational purposes, while, in contrast, ”information security” approaches consider all risks whether from internal or external sources. There can also be a perception that cybersecurity risks are primarily related to antagonistic threats, and that a lack of “cybersecurity” can create worse consequences to the organization than a lack of “information security”. Thus, cybersecurity can be perceived as more relevant to the organization than information security. This perception can cause confusion and also reduces the effectiveness of risk assessment and treatment.

Regardless of perception, the concepts behind information security can be used to assess and manage cybersecurity risks. The key question is how to manage cybersecurity risk in a comprehensive and structured manner, and ensure that processes, governance and controls exist and are fit for purpose. This can be done through a management systems approach. An Information Security Management System (ISMS) as described in ISO/IEC 27001 is a well proven way for any organization to implement a risk-based approach to cybersecurity.

This document demonstrates how a cybersecurity framework can utilize current information security standards to achieve a well-controlled approach to cybersecurity management.

Information technology — Security techniques — Cybersecurity and ISO and IEC Standards

1 Scope

This document provides guidance on how to leverage existing standards in a cybersecurity framework.

2 Normative references

There are no normative references in this document.

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at http://www.electropedia.org/

3.1
information security
preservation of confidentiality, integrity and availability of information

[SOURCE: ISO/IEC 27000:2016 2.33]

4 Document structure

This document provides background on the reasons why having a risk-based, prioritized, flexible, outcome-focused, and communications-enabling framework for cybersecurity is important. It then describes the objectives of a strong cybersecurity framework and includes mapping to existing standards that can be used to achieve these objectives.

5 Background

5.1 General

Cybersecurity is a relatively new discipline. ISO, IEC, and ISO/IEC standards developed over the last 25 years can be applied to help solve the challenges of cybersecurity. Existing and emerging cybersecurity frameworks throughout the world reference ISO, IEC, and ISO/IEC standards as useful sources of information.

Implementing cybersecurity framework, or a cybersecurity programme, requires a consistent and iterative approach to identifying, assessing, and managing risk and evaluating implementation of the framework. ISO/IEC 27001 already provides a risk management framework that can be applied to prioritize and implement cybersecurity activities within an organization.

5.2 Advantages of a risk-based approach to cybersecurity

A risk-based approach to cybersecurity:

— enables organizations to measure the impact of cybersecurity investments and improve their cybersecurity risk management over time;

— is prioritized, flexible, and outcome-focused;

— enables organizations to make security investment decisions that address risk, implement risk mitigations in a way that is most effective for their environments, and advance security improvements and innovations;

— facilitates communication across boundaries, both within and between organizations;

— is responsive to the actual risks faced by an organization, while recognizing that organizational resources are limited;

— reflects a clear understanding of the organization's particular business drivers and security considerations;

— allows an organization to manage risks in ways that are consistent with their own business priorities;

— enables organizations to have flexibility in a rapidly changing technology and threat landscape, and helps to address the varying needs of organizations and sectors.

More detailed and prescriptive guidance (e.g. detailed standards and guidelines) required by specific stakeholders for specific purposes can be provided on demand. Organizations that implement a risk-based cybersecurity framework can therefore take advantage of the benefits without being limited by the need for a full set of detailed implementation guidance.

5.3 Stakeholders

Stakeholders need to play an active role, beyond protecting their own assets, in order for the organization to realize the benefits of a connected global environment. Internet-enabled systems and applications are expanding beyond the business-to-business, business-to-consumer, and consumer-to-consumer models, to include many-to-many interactions and transactions. Individuals and organizations need to be prepared to address emerging security risks and challenges and effectively prevent and respond to misuse and criminal exploitation.

5.4 Activities of a cybersecurity framework and programme

The activities of a cybersecurity framework and programme are:

a) describe the organization's current cybersecurity status;

b) describe the organization's target state for cybersecurity;

c) identify and prioritize opportunities for improvement;

d) assess progress toward the target state;

e) communicate among internal and external stakeholders about cybersecurity risk.

6 Concepts

6.1 Overview of cybersecurity frameworks

A cybersecurity framework captures a set of desired cybersecurity outcomes that are common across all sectors and organizations. A framework facilitates communication about implementation of these desired outcomes and associated cybersecurity activities across the organization, from the executive level to the implementation and operations levels. The framework should consist of five functions, or high-level descriptions of desired outcomes, which are concurrent and continuous:

— Identify;

— Protect;

— Detect;

— Respond;

— Recover.

When considered together, these functions provide a high-level, strategic view of an organization's management of cybersecurity risk. Within each function, there are also categories and sub-categories, a prioritized set of activities that are important for achieving the specified outcomes.

Categories are the subdivisions of a function into groups of cybersecurity outcomes closely tied to programmatic needs and particular activities. Sub-categories further divide a category into specific outcomes of technical and/or management activities. They provide a set of results that, while not exhaustive, help support achievement of the outcomes in each category.

Organizing a cybersecurity framework into multiple levels, such as functions, categories, and sub-categories, helps to enable communication across boundaries. While many executives can seek to understand and make investments to more effectively mitigate organizational risk at the level of functions, operational practitioners can benefit from the more nuanced description of desired outcomes at the category or sub-category level. Importantly, though, if high-level and more nuanced descriptions of outcomes are organized within a single reference point that uses a common language, communication between executives and practitioners is facilitated, supporting strategic planning.

NOTE Annex B provides an example of another cybersecurity framework.

6.2 Cybersecurity framework functions

6.2.1 Overview

Functions organize basic cybersecurity outcomes and activities at their highest level. Important functions to include in a framework, as noted previously, are:

— Identify;

— Protect;

— Detect;

— Respond;

— Recover.

Each of these functions represents an area that an organization can use to express how it manages cybersecurity risk. These functions aid in organizing activities, enabling risk management decisions, addressing threats, and improving by learning from previous experiences.

The Identify function develops the organizational understanding to manage cybersecurity risk to systems, assets, data and capabilities. The activities in the Identify function are foundational for effective use of the framework. Understanding the business context, the resources that support critical functions, and the related cybersecurity risks enables an organization to focus and prioritize its efforts, consistent with its risk management strategy and business needs.

The Protect function develops and implements the appropriate safeguards to ensure delivery of critical infrastructure services. The Protect function supports the ability to limit or contain the impact of a potential cybersecurity event.

The Detect function develops and implements the appropriate activities to identify the occurrence of a cybersecurity event. The Detect function enables timely discovery of cybersecurity events.

The Respond function develops and implements the appropriate activities to take action regarding a detected cybersecurity event. The Respond function supports the ability to contain the impact of a potential cybersecurity event.

The Recover function develops and implements the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event.

Annex A examines each of the categories and breaks them down into possible outcomes and activities (sub-categories), demonstrating how to leverage existing ISO and IEC standards to better support the implementation of relevant activities.

6.3 Identify

The Identify function develops organizational understanding to manage cybersecurity risk to systems, assets, data and capabilities. The activities in the Identify function are important for effective use of the framework. Understanding the business context, the resources that support critical functions, and the related cybersecurity risks enables an organization to focus and prioritize its efforts, consistent with its risk management strategy and business needs. Within this function, there are activities that are vital to successful cyber risk management. To be able to identify these activities, an organization should understand its organisational objectives and risk management strategy.

Within the Identify function, the categories that can be included are:

Table 1 — Identify categories

Category	Description	References
Business environment	The organization's objectives, stakeholders, and activities are understood and used to inform roles, responsibilities and risk management decisions. Comprehensive security measures are necessary covering the company itself, its group companies, business partners of its supply chain and IT system control outsourcing companies.	ISO/IEC 27001:2013, Clause 4 ISO/IEC 27001: 2013, Clause 5 ISO/IEC 27036 (all parts) ISO/IEC 20243:2015, Clause 4 IEC 62443-2-1:2010, 4.2.1 ISO 31000:2009, 5.3
Risk assessment	The organization understands the risks to the organization's operations and assets. The management are required to drive cybersecurity risk measures considering any possible risk while in proceeding with the utilization of IT.	ISO/IEC 27001:2013, Clause 6 ISO/IEC 27014 ISO/IEC 20243:2015, Clause 4 IEC 62443-2-1:2010, 4.2 ISO 31000 ISO/IEC 38505
Risk management strategy	An organization's approach, the management components and resources to be applied to the management of risk.	ISO/IEC 27001:2013, 9.3 ISO/IEC 20243:2015, Clause 4 ISO 31000, Clause 4
Governance	To monitor and manage the organization's regulatory, legal, environmental and operational requirements. This information is then used to inform the appropriate levels of management.	ISO/IEC 27002:2013, Clause 5 ISO/IEC 27002:2013, Clause 6 ISO/IEC 38054 ISO/IEC 38505-1 ISO/IEC 20243:2015, Clause 4 IEC 62443-2-1:2010, 4.3.2.3
Asset Management	Identification and management of the systems, data, devices, people and facilities in relation to the business.	ISO/IEC 27002:2013 ISO/IEC 20243:2015, Clause 4 IEC 62443-2-1:2010, 4.2.3.4 ISO/IEC 27019:2017, Clause 7

6.4 Protect

The Protect function develops and implements appropriate safeguards to ensure delivery of resilient products and services. The Protect function also supports the ability to limit or contain the impact of a potential cybersecurity event.

Within the Protect function, the categories that can be included are:

Table 2 — Protect categories

Category	Description	References
Access control	Limiting access to facilities and assets to only authorized entities and associated activities. Included in access management is entity authentication	ISO/IEC 27002:2013, Clause 9 ISO/IEC 29146 ISO/IEC 29115 IEC 62443-2-1:2010, 4.3.3.5
Awareness and training	Ensuring users and stakeholders are aware of policies, procedures, and responsibilities relating to cybersecurity responsibilities.	ISO/IEC 27002:2013, Clause 6, 7 ISO/IEC 20243:2015, Clause 4 IEC 62443-2-1:2010, 4.3.2.4.2
Data security	Responsible for the confidentiality, integrity, and availability of data and information.	ISO/IEC 27002:2013, Clause 8
Information protection processes and procedures	Security policies, processes, and procedures are maintained and used to manage protection of information systems.	ISO/IEC 27002:2013
Maintenance	Processes and procedures for ongoing maintenance and modernization	ISO/IEC 27002:2013, Clause 11 ISO/IEC 20243:2015, Clause 4 IEC 62443-2-1:2010, 4.3.3
Protective technology	Technical security solutions (such as logging, removable media, least access principles, and network protection)	ISO/IEC 27002: 2013 ISO/IEC 27033 series IEC 62443-2-1:2010,

Annex A examines each of the categories and breaks them down into possible outcomes and activities (sub-categories), demonstrating how to leverage existing ISO and IEC standards to better support the implementation of relevant activities.

6.5 Detect

The Detect function identifies the occurrence of a cybersecurity event in a timely fashion.

Within the Detect function, the categories that can be included are:

Table 3 — Detect categories

Category	Description	References
Anomalies and events	Detection of anomalies and events and understanding of the impact of those events.	ISO/IEC 27002:2013, Clause 16 ISO/IEC 27035 (all parts) IEC 62443-2-1:2010, 4.3.4.5
Security continuous monitoring	Systems being monitored on a regular basis to validate the effectiveness of security measures in place.	ISO/IEC 27002:2013, Clause 12
Detection process	Processes and procedures to ensure timely awareness and communication of events.	ISO/IEC 27002:2013, Clause 16 ISO/IEC 27035 (all parts) IEC 62443-2-1:2010, 4.3.4.5

Annex A of this document examines each of the categories and breaks them down into possible outcomes and activities (sub-categories), demonstrating how to leverage existing ISO and IEC standards to better support the implementation of relevant activities.