TECHNICAL SPECIFICATION

ISO/IEC TS 27110

First edition
2021-02

Information technology, cybersecurity and privacy protection — Cybersecurity framework development guidelines

Sécurité de l'information, cybersécurité et protection de la vie privée — Lignes directrices relatives à l'élaboration d'un cadre en matière de cybersécurité

Reference number
ISO/IEC TS 27110:2021(E)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.

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 document 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 and IEC 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) or the IEC list of patent declarations received (see patents.iec.ch).

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

For an explanation of 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 www.iso.org/iso/foreword.html.

This document was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *Information security, cybersecurity and privacy protection*.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

Introduction

Cybersecurity is a pressing issue due to the use of connected technologies. Cyber threats are continually evolving, thus protecting users and organizations is a constant challenge. To cope with this challenge, business groups, government agencies, and other organizations produce documents and tools called cybersecurity frameworks to help organize and communicate cybersecurity activities of organizations. These organizations producing the cybersecurity frameworks are referred to as "cybersecurity framework creators." Other organizations and individuals then use or reference the cybersecurity framework in their cybersecurity activities.

Given that there are multiple cybersecurity framework creators, there are a multitude of cybersecurity frameworks. The current set of cybersecurity frameworks is diverse and varied. Organizations using cybersecurity frameworks are challenged with harmonizing different lexicons and conceptual structures to meet their requirements. These cybersecurity frameworks then become competing interests for finite resources. The additional effort could be better spent implementing cybersecurity and combating threats.

The goal of this document is to ensure a minimum set of concepts are used to define cybersecurity frameworks to help ease the burden of cybersecurity framework creators and cybersecurity framework users.

As this document limits itself with a minimum set of concepts, its length is kept to a minimum on purpose. This document is not intended to supersede or replace the requirements of an ISMS given in ISO/IEC 27001.

The principles of this document are as follows:

— flexible — to allow for multiple types of cybersecurity frameworks to exist;

— compatible — to allow for multiple cybersecurity frameworks to align; and

— interoperable — to allow for multiple uses of a cybersecurity framework to be valid.

The audience of this document is cybersecurity framework creators.

Information technology, cybersecurity and privacy protection — Cybersecurity framework development guidelines

1 Scope

This document specifies guidelines for developing a cybersecurity framework. It is applicable to cybersecurity framework creators regardless of their organizations' type, size or nature.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 27000, *Information technology — Security techniques — Information security management systems — Overview and vocabulary*

ISO/IEC TS 27100, *Information technology — Cybersecurity — Overview and concepts*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 27000, ISO/IEC TS 27100 and the following 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
cybersecurity framework
basic set of concepts used to organize and communicate cybersecurity activities

3.2
cyber persona
digital representation of an individual or organization necessary to interact in cyberspace

[SOURCE: U.S. DoD Joint Publication 3-12 and Caire, J, & Conchon, S:2016]

3.3
asset
anything that has value to an individual, an organization or a government

[SOURCE: ISO/IEC 27032:2012, 4.6, modified — The Note has been removed.]

4 Overview

Cybersecurity framework creators face a unique challenge: create a framework which is general enough to allow for flexibility in use while providing a structure to allow for compatibility and interoperability across frameworks and uses. Striking a balance between flexibility and compatibility while satisfying stakeholder requirements can be difficult. Developing multiple cybersecurity frameworks using the

same structure will help cybersecurity framework users maximize resources, while providing a way for different uses of a cybersecurity framework to achieve interoperability.

To help ease the challenge of creating a cybersecurity framework, this document provides the minimum set of concepts a cybersecurity framework should have: Identify, Protect, Detect, Respond, and Recover. This document can be used to build a framework of the minimum set of cybersecurity concepts.

While cybersecurity framework creators are subject to their unique stakeholder requirements, as shown in Figure 1, these concepts can also be used as pillars to help a cybersecurity framework creator structure and start filling out its lower level concepts. Unique stakeholder requirements can result in the creation of additional concepts to be contained in the resultant cybersecurity framework. However, the concepts presented in this document remain foundational.

Structured within these concepts, the resultant cybersecurity framework can consist of standards, guidelines, and practices to promote cybersecurity risk management. Cybersecurity frameworks provide prioritized, flexible, repeatable, and cost-effective approaches to help cybersecurity framework users manage cyber risk.

A cybersecurity framework helps persons executing these activities by providing a reference scheme. Concepts and categories of a cybersecurity framework can be used as a guide, checklist or template applicable in these activities.

A cybersecurity framework is not required in the implementation of an ISMS (ISO/IEC 27001). While ISO/IEC 27001 and a cybersecurity framework are independent, the two approaches can be related. Cybersecurity frameworks can be used in conjunction with ISMSs to organize cybersecurity activities across multiple layers of an organization, communicate those activities outside of the organization, and ensure continuous improvement of those activities over time. When a cybersecurity framework user chooses to implement an ISMS in conjunction with a cybersecurity framework, the two approaches work together to allow effective implementation of information security and cybersecurity activities, organization of those activities, and communication of those activities. An example of a cybersecurity framework and an ISMS working together is presented in Annex A. Considerations on the integration of a cybersecurity framework into practice are provided in Annex B. Examples of cybersecurity framework are listed in the Bibliography.

Many cybersecurity frameworks implement the concept of risk management, but not all. Cybersecurity frameworks should consider the concept of risk management.

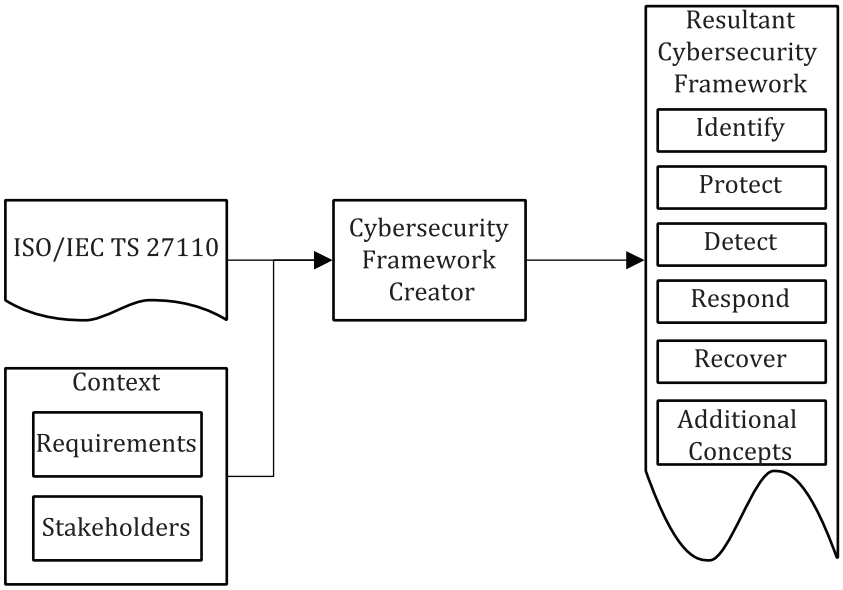

Figure 1 — Creating a cybersecurity framework using ISO/IEC TS 27110

The value of applying the guidelines in this document is that users of different cybersecurity frameworks can communicate with each other. These concepts are intended to give a cybersecurity framework creator a starting point, and when used collectively, provide an effective structure in organizing a cybersecurity framework.

5 Concepts

5.1 General

The purpose of subclauses 5.2 to 5.6 is to describe the concepts in a cybersecurity framework. These concepts are intended to give a cybersecurity framework creator a starting point. While every cybersecurity framework has different stakeholders and requirements, the concepts below remain constant and, thus, serve as the basis for any cybersecurity framework.

The concepts listed below are not intended to provide sufficient detail for implementation of cybersecurity within an organization. These concepts can be arranged in a process model. However, other configurations can work given the cybersecurity framework creator's stakeholder requirements.

Cybersecurity framework creators can choose to augment the cybersecurity framework with additional concepts which provide value to their stakeholders or satisfy specific requirements. Furthermore, some cybersecurity framework creators can choose to enhance these concepts with categories and subcategories to provide more guidance to their stakeholders or satisfy requirements. Some contexts can warrant a greater level of detail than categories. If that is the case, cybersecurity framework creators may specify additional, more detailed statements that would align at the subcategory level.

The concepts presented below are independent of time, context, granularity of scope, and market conditions. While sequence of events, unique operating constraints, and business drivers are all important factors when designing a cybersecurity framework, they are considered implementation details.

5.2 Identify

A cybersecurity framework should include the Identify concept.

The Identify concept develops the ecosystem of cybersecurity which is being considered.

This ecosystem is used when developing the Protect, Detect, Respond and Recover concepts. Examples of ecosystem considerations are: business objectives, business environment, stakeholders, assets, business processes, laws, regulations, threat environment and cyber risks. The Identify concept addresses people, policies, processes and technology when defining the scope of activities. The Identify concept can include many categories relating to scoping particular activities to only those which are relevant. Categories can include: business environment, risk assessment, risk management strategy, governance, asset management, business context analysis and supply chain considerations.

The activities in scope of the Identify concept are foundational for cybersecurity. The Identify concept can include an understanding of business context, stakeholders, the cybersecurity ecosystem and dependencies. An organization's presence in cyberspace, its cyber persona, the business-critical functions and information and their related resources can also be important. The understanding gained from the Identify concept enables a flexible and repeatable view of cybersecurity for an organization to focus and prioritize its efforts.

A cybersecurity framework creator should consider evolving cyber threats and emerging technology when designing the Identify concept. Otherwise, the resulting cybersecurity framework can fail to appropriately meet future requirements.

5.3 Protect

A cybersecurity framework should include the Protect concept.

The Protect concept develops appropriate safeguards to protect an organization's cyber persona, ensure preventative controls are working, and produce the desired readiness of the organization to deliver critical services and maintain its operations and security of its information.

The Protect concept can contain many categories and activities related to the safeguarding of assets against intentional or unintentional misuse. The Protect concept can include controls for traditional IT system security, industrial control systems or internet of things. Categories can include: access control, awareness and training, data security, information protection processes and procedures, maintenance, protective technology, security architecture, asset configuration, systems segregation, traffic filtering, cryptography, security administration and maintenance, identity and access management and data security.

A cybersecurity framework creator should determine the scope of the Protect concept. Prevention and threat-oriented approaches can be used. When developing the Protect concept, a cybersecurity framework creator should consider protection for people, process and technology.

5.4 Detect

A cybersecurity framework should include the Detect concept.

The Detect concept develops the appropriate activities to discover cybersecurity events.

The activities in the Detect concept provide an organization the ability to proactively observe changes in behaviours, states, traffic, configuration or processing of its key resources. These changes can be internal or external, intentional or unintentional. By understanding the changing landscape, the organization can make updates to policies, procedures and technology as needed.

The Detect concept can include traditional asset monitoring and attack detection. Categories can include: anomalies and events, security continuous monitoring, detection process, logging, log correlation and analysis, threat hunting, anomaly detection and operational baseline creation.

A cybersecurity framework creator should consider the depth and scope of internal and external changes to be observed. Increasing scope of the Detect concept can add value to a cybersecurity framework as well as potential additional burden. Some cybersecurity frameworks can focus on the system level while others focus on process level. When considering the Detect concept, cybersecurity framework creators should determine the appropriate level of detail to guide organizations.

5.5 Respond

A cybersecurity framework should include the Respond concept.

The Respond concept develops the appropriate activities regarding the response to cybersecurity events.

The activities in the Respond concept allow an organization to qualify the cybersecurity events in their environment and react to them. These activities allow an organization to categorize, evaluate, and remediate cybersecurity events based on their specific needs, resources, stakeholders and requirements.

The Respond concept can include the traditional incident response concepts as well as policies, procedures and plans. Categories can include: response planning, communications, analysis, mitigation, improvements, incident response, environment sterilization or malware eradication.

A cybersecurity framework creator should consider the broader context of the Respond concept, e.g. managerial and procedural aspects. In addition to incident response, the Respond concept can incorporate communication to and from external parties. These communications can be vulnerability disclosures, threat reports or other information provided by external sources. Additionally, the Respond concept can include the sharing of information with external sources. A cybersecurity framework creator should consider the entire ecosystem in which the cybersecurity framework will be deployed to understand the Respond concept.

5.6 Recover

A cybersecurity framework should include the Recover concept.

The Recover concept develops the appropriate activities to restore services, repair systems and restore reputation.

The activities in the Recover concept define the restoration and communication related activities after a cybersecurity event. The Recover concept is not only a reactive concept, but also a proactive concept. Effective and efficient planning and execution of the activities in the Recover concept should minimize damage and help organizations resume operations.

It is possible that services have been degraded during a cybersecurity incident. The Recover concept is an opportunity to provide guidance on how to restore those services. Services can be technical or managerial processes in nature. Assets can have reached an inoperable or undesired state of operation. The Recover concept is an opportunity to provide guidance on how to repair those assets. Reputation can have been damaged during a cybersecurity incident. Reputation can be a key factor in maintaining market share or consumer confidence. Categories can include: recovery planning, communications, improvements, recovery training and recovery execution.

A cybersecurity framework creator should consider a number of factors influencing priority of service restoration when producing a cybersecurity framework. These include business impact, stakeholder needs, implementation scenarios and technological maturity. While some cybersecurity frameworks do not incorporate business goals, the non-technical ramifications of a recovery can be severe and can be addressed by a cybersecurity framework.

6 Creating a cybersecurity framework

Cybersecurity framework creators should use Identify, Protect, Detect, Respond and Recover concepts to structure and organize desired cybersecurity and information security activities into a cybersecurity framework. As shown in Figure 1, the cybersecurity and information security activities to be organized into a cybersecurity framework depend on the context and requirements that guide cybersecurity framework creators. Once all activities are identified, they should be organized under the concepts and then, if needed, split into categories and subcategories depending on the desired level of detail. If an additional level of detail is desired, cybersecurity framework creators can add more detailed statements to align at the subcategory level.