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.

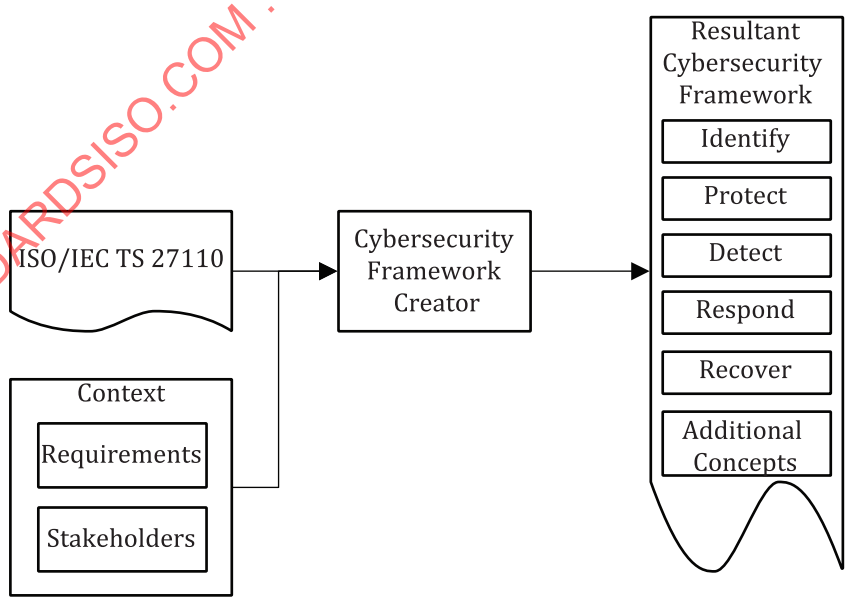

Figure 1 — Creating a cybersecurity framework using ISO/IEC TS 27110

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.

Annex A
(informative)

Considerations in the creation of a cybersecurity framework

A.1 General

The considerations proposed in this annex aim to guide cybersecurity framework creators in designing a cybersecurity framework.

While there can be other interpretations of the concepts and standards listed, A.2 to A.4 are presented as a compendium of three examples.

Example 1 is a replication of ISO/IEC TR 27103 which demonstrates a cybersecurity framework created from selected ISO/IEC standards. This example provides additional categories which are a further subdivision of the base concepts. While categories within a specific concept can vary, concepts remain constant per this document. Tables A.1 to A.5 show example categories and references within each concept.

Example 2 is also a replication of ISO/IEC TR 27103 which demonstrates a cybersecurity framework created from selected ISO/IEC standards. While categories within a specific concept can vary, concepts remain constant per this document. This example provides an additional layer of specification with both categories and subcategories. Tables A.6 to A.27 show example categories, subcategories and references within each category.

Example 3 is a generic cybersecurity framework which is does not reference other standards or guidance. This cybersecurity framework specifies categories within each concept and subcategories within each category.

A.2 Example 1

Table A.1 — Example categories and references within Identify

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)
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

Table A.1 *(continued)*

Category	Description	References
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
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
Asset Management	Identification and management of the systems, data, devices, people and facilities in relation to the business.	ISO/IEC 27002:2013 ISO/IEC 27019:2017, Clause 7

Table A.2 — Example categories and references within Protect

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
Awareness and training	Ensuring users and stakeholders are aware of policies, procedures, and responsibilities relating to cybersecurity responsibilities.	ISO/IEC 27002:2013, Clauses 6 and 7
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
Protective technology	Technical security solutions (such as logging, removable media, least access principles, and network protection)	ISO/IEC 27002:2013 ISO/IEC 27033 (all parts)

Table A.3 — Example categories and reference within Detect

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)
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)

Table A.4 — Example categories and references within Respond

Category	Description	References
Response planning	Plan for how to respond to events in a timely manner including processes and procedures for responding to events.	ISO/IEC 27002:2013, Clause 16 ISO/IEC 27035 (all parts)
Communications	Processes and procedures for communicating the timely information to relevant parties. Companies need to communicate appropriately with relevant parties by, for example, disclosing information on security measures or response on regular basis or in times of emergency.	ISO/IEC 27002:2013, Clause 16 ISO/IEC 27035 (all parts) ISO/IEC 27014
Analysis	Review of detected events, including categorization and impact of events.	ISO/IEC 27002:2013, Clause 16 ISO/IEC 27035 (all parts)
Mitigation	Activities that limit the expansion of the event, mitigate the event and stop the event.	ISO/IEC 27002:2013, Clause 16 ISO/IEC 27035 (all parts)
Improvements	Organization reviews the response plan and improves it based on lessons learned during an event.	ISO/IEC 27002:2013, Clause 16 ISO/IEC 27035 (all parts)

Table A.5 — Example categories and references within Recover

Category	Description	References
Recovery planning	Plan for how to recover from an event and the next steps after an event.	ISO/IEC 27002:2013, Clause 16 ISO/IEC 27035 (all parts)
Communications	Processes and procedures for communicating the timely information to relevant parties.	ISO/IEC 27002:2013, Clause 16 ISO/IEC 27035 (all parts)
Improvements	Organization takes the lessons learned during an event and feeds it back into the process and procedures.	ISO/IEC 27002:2013, Clause 16 ISO/IEC 27035 (all parts)

A.3 Example 2

Table A.6 describes the activities under the business environment category, along with standards that can support the understanding and implementation of these activities.

Table A.6 — Identify concept: business environment category, subcategories, and references

Description of subcategory	Standards mapping
The organization's role in the supply chain is identified and communicated	ISO/IEC 27002:2013, 15.1.3, 15.2.1 ISO/IEC 27036-1 ISO/IEC 20243:2015, Clause 4
The organization's place in critical infrastructure and its industry sector is identified and communicated	ISO/IEC 27001:2013, 4.1
Priorities for organizational mission, objectives, and activities are established and communicated	ISO/IEC 27002:2013, Clause 6

Table A.6 *(continued)*

Description of subcategory	Standards mapping
Dependencies and critical functions for delivery of critical services are established	ISO/IEC 27002:2013, 11.2.2 ISO/IEC 27019:2017, 9.2.2, 9.2.3, 10.11.1
Resilience requirements to support delivery of critical services are established	ISO/IEC 27002:2013, 11.1.4, 17.1.1 ISO/IEC 27019:2017, 10.12.1

Table A.7 describes the activities under the risk assessment category, along with standards that can support the understanding and implementation of these activities.

Table A.7 — Identify concept: risk assessment category, subcategories, and references

Description of subcategory	Standards mapping
Asset vulnerabilities are identified and documented	ISO/IEC 27002:2013, 12.6.1, 18.2.3 ISO/IEC 29147 ISO/IEC 27019:2017, 7.1.1, 7.1.2
Threat and vulnerability information is received from information sharing forums and sources	ISO/IEC 27002:2013, 6.1.4
Internal and external threats are identified and documented	ISO/IEC 27001:2013, 6.1.2
Potential business impacts and likelihoods are identified	ISO/IEC 27001:2013, 6.1.2
Threats, vulnerabilities, likelihoods, and impacts are used to determine risk	ISO/IEC 27002:2013, 12.6.1
Risk responses are identified and prioritized	ISO/IEC 27001:2013, 6.1.3

Table A.8 describes the activities under the risk management strategy category, along with standards that can support the understanding and implementation of these activities.

Table A.8 — Identify concept: risk management strategy category, subcategories, and references

Description of subcategory	Standards mapping
Risk management processes are established, managed, and agreed to by organizational stakeholders	ISO/IEC 27001:2013, 6.1.3, 8.3,9.3
Organizational risk tolerance is determined and clearly expressed	ISO/IEC 27001:2013, 6.1.3, 8.3
The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis	ISO/IEC 27001:2013, 6.1.3, 8.3

Table A.9 describes the activities under the governance category, along with standards that can support the understanding and implementation of these activities.

Table A.9 — Identify concept: governance category, subcategories, and references

Description of subcategory	Standards mapping
Information security policy for the organization is established	ISO/IEC 27002:2013, 5.1.1
Information security roles & responsibilities are coordinated and aligned with internal roles and external partners	ISO/IEC 27002:2013, 6.1.1, 7.2.1
Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed	ISO/IEC 27002:2013, 18.1
Governance and risk management processes address cybersecurity risks	ISO/IEC 27001:2013, Clause 6

The category of asset management covers any data, personnel, devices, systems or facilities that are used or managed by the organization. Asset management covers the physical inventory of devices and

systems, inventory of software platforms and applications in an organization and the mapping of the data flows. ISO/IEC 27001:2013, Annex A, describes controls that can assist with knowing if the activity has been completed. ISO/IEC 27002 provides guidance for implementation of those controls. Some of the subcategories and standards that already exist to help with those subcategories are identified in Table A.10.

Table A.10 — Identify concept: asset management category, subcategories, and references

Description of subcategory	Standards mapping
Physical devices and systems within the organization are inventoried	ISO/IEC 27002:2013, 8.1.1, 8.1.2 ISO/IEC 27019:2017, 9.2.1
Software platforms and applications within the organization are inventoried	ISO/IEC 27002:2013, 8.1.1, 8.1.2
Organizational communication and data flows are mapped	ISO/IEC 27002:2013, 13.2.1
External information systems are catalogued	ISO/IEC 27002:2013, 11.2.6, 8.2.1
Resources (e.g. hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value	ISO/IEC 27002:2013, 11.2.6, 8.2.1

Table A.11 describes the activities under the access control category, along with standards that can support the understanding and implementation of these activities.

Table A.11 — Protect concept: access control category, subcategories, and references

Description of subcategory	Standards mapping
Identities and credentials are managed for authorized devices and users	ISO/IEC 27002:2013, 9.2.1, 9.2.2, 9.2.4, 9.2.5, 9.2.6, 9.3.1, 9.4.2, 9.4.3 ISO/IEC 27019:2017, 11.1.1, 11.3.1, 11.5.2
Physical access and remote access are managed and protected	ISO/IEC 27002:2013, 11.1.1, 11.1.2, 6.2.2, 13.1.1
Manage access permissions use the least principle and separation of duties	ISO/IEC 27002:2013, 6.1.2, 9.1.2, 9.2.3, 9.4.1, 9.4.4 ISO/IEC 27019:2017, 8.1.1
Network integrity is protected, including network segregation as appropriate	ISO/IEC 27002:2013, 13.1.1, 13.1.3 ISO/IEC 27033-2 ISO/IEC 27033-3 ISO/IEC 27019:2017, 10.6.3, 11.4.5, 11.4.8

Table A.12 describes the activities under the awareness and training category, along with standards that can support the understanding and implementation of these activities.

Table A.12 — Protect concept: awareness and training category, subcategories, and references

Description of subcategory	Standards mapping
All users are informed and trained	ISO/IEC 27002:2013, 7.2.2
Roles and responsibilities of senior executives, privileged users, stakeholders, personnel (physical and information security) and third-party stakeholders (e.g. suppliers, customers, partners) are understood	ISO/IEC 27002:2013, 7.2.1, 7.2.2, 6.1.1, 8.2.1

Table A.13 describes the activities under the data security category, along with standards that can support the understanding and implementation of these activities.

Table A.13 — Protect concept: data security category, subcategories, and references

Description of subcategory	Standards mapping
Data at rest is protected	ISO/IEC 27002:2013, 8.2.3 ISO/IEC 27033-2 ISO/IEC 27040
Data-in-transit is protected	ISO/IEC 27002:2013, 8.2.3, 13.1.1, 13.2.1, 13.2.3, 14.1.2, 14.1.3 ISO/IEC 27033-2 ISO/IEC 27033-5
Assets are formally managed throughout removal, transfers and disposition	ISO/IEC 27002:2013, 8.2.3, 8.3.1, 8.3.2, 8.3.3, 11.2.7
Appropriate capacity planning to ensure availability	ISO/IEC 27002:2013, 12.1.3, 12.3.1
Data leakage protection	ISO/IEC 27002:2013, 6.1.2, 7.1.1, 7.1.2, 7.3.1, 8.2.2, 8.2.3, 9.1.1, 9.1.2, 9.2.3, 9.4.1, 9.4.4, 9.4.5, 13.1.3, 13.2.1, 13.2.3, 13.2.4, 14.1.2, 14.1.3
Integrity checking mechanisms are used to verify software, firmware, and information integrity	ISO/IEC 27002:2013, 12.2.1, 12.5.1, 14.1.2, 14.1.3
The development and testing environment(s) are separate from the production environment	ISO/IEC 27002:2013, 12.1.4 ISO/IEC 27019:2017, 10.1.4

Table A.14 describes the activities under the information protection processes and procedures category, along with standards that can support the understanding and implementation of these activities.

Table A.14 — Protect concept: information protection processes and procedures category, subcategories, and references

Description of subcategory	Standards mapping
Baseline configurations of systems are created and maintained	ISO/IEC 27002:2013, 12.1.2, 12.5.1, 12.6.2, 14.2.2, 14.2.3, 14.2.4 ISO/IEC 27019:2017, 12.1.1
A system development life cycle to manage systems is implemented	ISO/IEC 27002:2013, 6.1.5, 14.1.1, 14.2.1, 14.2.5 ISO/IEC 27034 (all parts)
Change control process in place	ISO/IEC 27002:2013, 12.1.2, 12.5.1
Backups are conducted, maintained and tested	ISO/IEC 27002:2013, 12.3.1
Physical operating environment meets policy and regulations for organizational assets	ISO/IEC 27002:2013, 11.1.4, 11.2.1, 11.2.2, 11.2.3 ISO/IEC 27019:2017, 9.1.1, 9.1.2, 9.2.3, 9.1.7, 9.1.8, 9.1.9
Data destruction follows appropriate policy	ISO/IEC 27002:2013 8.2.3, 8.3.1, 8.3.2, 11.2.7
Protection processes are continuously improved	ISO/IEC 27001:2013, Clauses 9 and 10
Communication of effectiveness of protection technologies is shared with appropriate parties	ISO/IEC 27001:2013, 7.4 ISO/IEC 27002:2013, 16.1.6

Table A.14 *(continued)*

Description of subcategory	Standards mapping
Response and recovery plans are in place, managed and tested	ISO/IEC 27002:2013, 16.1.1, 17.1.1, 17.1.2 ISO/IEC 27031 ISO/IEC 27035-1 ISO/IEC 27035-2 ISO/IEC 27019:2017 14.1.1
Vulnerability management	ISO/IEC 27002:2013, 12.6.1, 18.2.2

Table A.15 describes the activities under the maintenance category, along with standards that can support the understanding and implementation of these activities.

Table A.15 — Protect concept: maintenance category, subcategories, and references

Description of subcategory	Standards mapping
Organizational assets are maintained and repaired following approved processes and tools	ISO/IEC 27002:2013, 11.1.2, 11.2.4
Remote maintenance is performed following approved processes and protected from unauthorized accesses.	ISO/IEC 27002:2013, 11.2.4, 15.1.1, 15.2.1

Table A.16 describes the activities under the protective technology category, along with standards that can support the understanding and implementation of these activities.

Table A.16 — Protect concept: protection technologies category, subcategories, and references

Description of subcategory	Standards mapping
Audit/log records are determined, documented, implemented, and reviewed in accordance with policy	ISO/IEC 27002:2013, 12.4.1, 12.4.2, 12.4.3, 12.4.4, 12.7.1 ISO/IEC 27019:2017, 10.10.1
Removable media follows appropriate policy	ISO/IEC 27002:2013, 8.2.2, 8.3.1, 8.3.3 ISO/IEC 27040
Principle of least functionality is applied to access to systems and assets	ISO/IEC 27002:2013, 9.1.2
Communications and control networks are protected	ISO/IEC 27002:2013, 13.1.1, 13.2.1 ISO/IEC 27033-2 ISO/IEC 27019:2017, 10.6.3

Table A.17 describes the activities under the anomalies and events category, along with standards that can support the understanding and implementation of these activities.

Table A.17 — Detect concept: anomalies and events category, subcategories, and references

Description of subcategory	Standards mapping
Baseline of network operations and data flows is established	ISO/IEC 27033 (all parts)
Detected events are analysed to understand attack targets and methods	ISO/IEC 27002:2013, 16.1.1, 16.1.4 ISO/IEC 27035 (all parts)
Event data is aggregated and correlated from multiple sources and sensors	ISO/IEC 27035 (all parts)
Determination of impact of event	ISO/IEC 27035 (all parts)
Alert thresholds are established	ISO/IEC 27035 (all parts)

Table A.18 describes the activities under the security continuous monitoring category, along with standards that can support the understanding and implementation of these activities.

Table A.18 — Detect concept: security continuous monitoring category, subcategories, and references

Description of subcategory	Standards mapping
Monitoring network, physical environment, personnel, and service provider for potential events	ISO/IEC 27002:2013, 12.4.1, 14.2.7, 15.2.1
Malicious code is detected	ISO/IEC 27002:2013, 12.2.1 ISO/IEC 27019:2017, 10.4.1
Unauthorized mobile code is detected	ISO/IEC 27002:2013, 12.5.1
Monitoring for unauthorized personnel, connections, devices, and software is performed	ISO/IEC 27002:2013, 12.4.1, 14.2.7, 15.2.1
External service provider activity is monitored to detect potential cybersecurity events	ISO/IEC 27036 (all parts)
Vulnerability scans are performed	ISO/IEC 27002:2013, 14.2.9

Table A.19 describes the activities under the detection processes category, along with standards that can support the understanding and implementation of these activities.

Table A.19 — Detect concept: detection processes category, subcategories, and references

Description of subcategory	Standards mapping
Roles and responsibilities for detection are well defined to ensure accountability	ISO/IEC 27002:2013, 6.1.1 ISO/IEC 27019:2017, 8.1.1
Detection activities comply with all applicable requirements	ISO/IEC 27002:2013, 18.1.4
Detection processes are tested	ISO/IEC 27002:2013, 14.2.8
Event detection information is communicated to appropriate parties	ISO/IEC 27002:2013, 16.1.2 ISO/IEC 27035 (all parts)
Detection processes are continuously improved	ISO/IEC 27002:2013, 16.1.6 ISO/IEC 27035 (all parts)

Table A.20 describes the activities under the response planning category, along with standards that can support the understanding and implementation of these activities.

Table A.20 — Respond concept: response planning category, subcategories, and references

Description of subcategory	Standards mapping
Response plan is executed during or after an event	ISO/IEC 27002:2013, 16.1.5 ISO/IEC 27035 (all parts)

Table A.21 describes the activities under the communications category, along with standards that can support the understanding and implementation of these activities.

Table A.21 — Respond concept: communications category, subcategories, and references

Description of subcategory	Standards mapping
Personnel know their roles and order of operations when a response is needed	ISO/IEC 27001:2013, 7.4 ISO/IEC 27002:2013, 6.1.1, 16.1.1 ISO/IEC 27035 (all parts) ISO/IEC 27019:2017, 6.1.6, 8.1.1

Table A.21 *(continued)*

Description of subcategory	Standards mapping
Events are reported consistent with established criteria	ISO/IEC 27001:2013, 7.4 ISO/IEC 27002:2013, 6.1.3, 16.1.2 ISO/IEC 27035 (all parts)
Information is shared consistent with response plans	ISO/IEC 27001:2013, 7.4 ISO/IEC 27002:2013, 16.1.2 ISO/IEC 27035 (all parts)
Coordination with stakeholders occurs consistent with response plans	ISO/IEC 27001:2013, 7.4 ISO/IEC 27002:2013, 6.1.4, 16.1.5 ISO/IEC 27033-2 ISO/IEC 27035 (all parts) ISO/IEC 27019:2017, 6.1.7
Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situation awareness	ISO/IEC 27001:2013, 7.4

Table A.22 describes the activities under the analysis category, along with standards that can support the understanding and implementation of these activities.

Table A.22 — Respond concept: analysis category, subcategories, and references

Description of subcategory	Standards mapping
Notifications from detection systems are investigated	ISO/IEC 27002:2013, 12.4.1, 12.4.3, 16.1.5 ISO/IEC 27039
The impact of the incident is understood	ISO/IEC 27002:2013, 16.1.6 ISO/IEC 27035-2
Forensics are performed	ISO/IEC 27002:2013, 16.1.7
Incidents are categorized consistent with response plans	ISO/IEC 27002:2013, 16.1.4

Table A.23 describes the activities under the mitigation category, along with standards that can support the understanding and implementation of these activities.

Table A.23 — Respond concept: mitigation category, subcategories, and references

Description of subcategory	Standards mapping
Incidents are contained and mitigated	ISO/IEC 27002:2013, 12.2.1, 16.1.5 ISO/IEC 27035-1 ISO/IEC 27035-2
Newly identified vulnerabilities are mitigated or documented as accepted	ISO/IEC 27002:2013, 12.6.1

Table A.24 describes the activities under the improvements category, along with standards that can support the understanding and implementation of these activities.

Table A.24 — Respond concept: improvements category, subcategories, and references

Description of subcategory	Standards mapping
Response plans incorporate lessons learned	ISO/IEC 27001:2013, Clause 10 ISO/IEC 27002:2013, 16.1.5, 16.1.6
Response strategies are updated	ISO/IEC 27001:2013, Clause 10 ISO/IEC 27002:2013, 16.1.6

Table A.25 describes the activities under the recovery planning category, along with standards that can support the understanding and implementation of these activities.

Table A.25 — Recover concept: recovery planning category, subcategories, and references

Description of subcategory	Standards mapping
Recovery plan is executed during or after an event	ISO/IEC 27002:2013, 16.1.5 ISO/IEC 27031

Table A.26 describes the activities under the improvements category, along with standards that can support the understanding and implementation of these activities.

Table A.26 — Recover concept: improvements category, subcategories, and references

Description of subcategory	Standards mapping
Recovery plans incorporate lessons learned	ISO/IEC 27001:2013, Clause 10 ISO/IEC 27031
Recovery strategies are updated	ISO/IEC 27001:2013, Clause 10 ISO/IEC 27031

Table A.27 describes the activities under the communications category, along with standards that can support the understanding and implementation of these activities.

Table A.27 — Recover concept: communications category, subcategories, and references

Description of subcategory	Standards mapping
Public relations are managed	ISO/IEC 27001:2013, 7.4 ISO/IEC 27019:2017, 14.2.1
Reputation after an event is repaired	ISO/IEC 27001:2013, 7.4
Recovery activities are communicated to internal stakeholders and executive and management teams	ISO/IEC 27001:2013, 7.4

A.4 Example 3

Identify

Table A.28 — Considerations of Identify

Category	Example of activities	Example of input	Example of output
Business environment	Understand the business environment and its ecosystem of internal and external stakeholders.	Research and interviews on relevant information sources and persons of reference	Document or a chapter presenting the identified stakeholders and their requirements relevant to cybersecurity
Context	Identify industry sectors, activities, functions, processes, cyber representation (cyber persona) and their stakeholders internal or external to the organization where cybersecurity is of importance.	Research on relevant information sources	Document or chapter inventorying the primary sectors of essential services, activities, functions, processes, cyber representation (cyber persona) and their stakeholders internal or external to the organization in scope at the desired level of granularity
Asset management	Identify assets or their categories of resources that support the previously identified sectors of essential services, functions, information and cyber representation (cyber persona). Adjust the level of the categories according to the size of the scope for which the framework is intended. Inventory the scopes of resources that are exposed to threats and that are eligible for cybersecurity protection.	Knowledge base of supporting assets. Context establishment document. Relevant reference(s): Threat knowledge base such as., MITRE CAPEC, EBIOS Identification of threats	Inventory of assets or their categories in the scope of the cybersecurity framework. The level of granularity should be adequate with respect to the size of the scope. Cross-check of assets potentially exposed to the identified threats
Risk assessment	Risk identification: Identify categories of risk sources from the ecosystem. Use knowledge bases, identify the threat operating modes potentially affecting these resources. Identify risk sources and their adverse effects on sectors of essential services, activities, functions, information, processes, cyber representations (cyber persona) and their stakeholders internal or external to the organization.	Threat observations, Incident sharing observations from security agencies or consulting companies	Document listing the risk sources relevant to the context

Table A.28 *(continued)*

Category	Example of activities	Example of input	Example of output
Governance	Identify authorities in charge of cybersecurity regulation and the related laws and regulations, security agencies in charge of observing threats, organizing the national cybersecurity ecosystem, identifying the industry sectors of essential services, the incident notification.	Available documentation about regulatory organization in the concerned geographical footprint of the scope	Document stating the constraints affecting the organization and the applicable legislative and regulatory references
Risk management strategy	Identify the chain of command related to risk treatment decision making, risk mitigation plans, budget allocation, crisis management, continuous improvement, business continuity.	Available documentation in the organization	Document stating the organization of risk management and the decision-making process for resource allocation in risk mitigation measures and risk monitoring
Supply chain	Identify critical assets and suppliers that provide products or services for those assets, relevant roles and responsibilities, processes, and artifacts.	Policies, plans, and procedures that identify and manage cyber risks associated with supply chain	Contractual security requirements; supplier monitoring regime; additional roles and responsibilities; communication channels and mechanisms between acquirer and supplier

For a wider overview of relevant International Standards contributing to the Identify concept, please refer to ISO/IEC TR 27103:2018. This example cybersecurity framework differs slightly from ISO/IEC TR 27103:2018 in its presentation. However, the content remains the same. This example demonstrates the flexibility and compatibility principles of this document.

Protect

Table A.29 — Considerations of Protect

Category	Example of activities	Example of input	Example of output
Prevention	Establish applicable cybersecurity baseline characteristics for the assets in scope. For example: IT security architecture (systems configuration, system segregation, traffic filtering, cryptography) IT security administration (administration accounts, administration information systems) Identity and access management including authentication, access rights, access control IT security maintenance Physical and environmental security Awareness and training Data security Information protection processes and procedures Maintenance Protective technology	Existing cybersecurity baseline characteristics that include robustness of architecture, robustness of systems configuration, systems segregation, traffic filtering, cryptography, IT security administration and maintenance, Identity and Access management, security of industrial control systems, data security	Selection of the relevant cyber security baseline characteristics to protect assets from the physical, logical, and cyber perspectives Set of security baselines covering the protection of technology, the awareness, training and skills of staff, the preventative security processes and procedures
Assessment	Establishment of principles to elaborate security assessment methods and execute assessment The independence of the experts that elaborates security assessment methods on products and services should be preserved from any vendor influence. Adequate skills and independence should be ensured to be in capacity to perform an assessment. Certifications schemes should be considered, accredited schemes.	Example of security assessment methods	Principles in the cybersecurity framework elaborating security assessment methods and executing assessment Principles in the cybersecurity framework establishing independence of the players in charge of elaborating assessment methods and executing assessment. Such independence should be effective against the manufacturers or vendors of the product and services being assessed.

Table A.29 *(continued)*

Category	Example of activities	Example of input	Example of output
Lifecycle security	Milestones should be considered to integrate security in the lifecycle of products and services. Two complementary approaches should be specified in the cybersecurity framework: on one hand security specifications at the entry of the lifecycle should complement functional specifications. The quality management of the lifecycle should deliver a product compliant with the security specification. On the other hand, security expertise should be involved with checking the design and implementation robustness of the product that make it resistant to attack methods. IT and network operations should be considered eligible to lifecycle processes.	Existing lifecycle methodologies Security in agile lifecycle frameworks	Products and services compliant with the security specifications

For a wider overview of relevant International Standards contributing to the Protect concept, please refer to ISO/IEC TR 27103:2018. This example cybersecurity framework differs slightly from ISO/IEC TR 27103:2018 in its presentation. However, the content remains the same. This example demonstrates the flexibility and repeatability principles of this document.

Detect