FINAL DRAFT
International Standard

ISO/FDIS 22340

Security and resilience — Protective security — Guidelines for an enterprise protective security architecture and framework

Sécurité et résilience — Sûreté préventive — Lignes directrices pour une architecture et un cadre de sûreté préventive de l'entreprise

ISO/TC **292**

Secretariat: **SIS**

Voting begins on:
2024-07-15

Voting terminates on:
2024-09-09

Reference number
ISO/FDIS 22340:2024(en)

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) 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 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).

ISO draws attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO takes no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO had not received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at www.iso.org/patents. ISO shall not be held responsible for identifying any or all such patent rights.

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 Technical Committee ISO/TC 292, *Security and resilience*.

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

This document aims to meet a global need for organizations to formulate and integrate their protective security controls in a way that is based on risk management principles and strategically aligned with the interests of the organization. It details an enterprise architecture and integrated framework within which a diverse suite of security-related policy, processes and practices can be coordinated.

Clarity on what protective security is, what it means, how it can be implemented, and how its benefits can be measured, will be helpful to managers, regardless of the sector. This is particularly important for the many organizations that have expended substantial resources on various security measures that have not necessarily been coordinated or informed by the full range of security risk. In an increasingly complex security environment, this document aims to provide clarity in this regard and to provide a basis for better enterprise security outcomes as a result.

This document:

a) Provides guidance on how organizations and their managers can implement and manage coherent protective security arrangements.

b) Demonstrates the critically important idea that effective security management is based on an understanding of risk and the application of risk management principles, and that the form and implementation of security controls (that protect an organization's assets) are integral to the long-term success of the organization. Security is a business enabler, not an overhead cost to the organization.

c) Defines and details the elements of protective security, outlines an enterprise protective security governance model and defines the roles and responsibilities necessary in delivering protective security outcomes.

d) Demonstrates the critical importance of establishing and sustaining an organizational culture supporting positive security behaviours: where all personnel and interested parties have a sense of shared ownership of security outcomes; and where all are authorized and competent to act in the security interests of the organization and invested in the security of the organization.

e) Outlines the importance of continuous improvement in relation to an organization's protective security.

This document is applicable for any organization and will be particularly useful for those that have had difficulty implementing risk-based frameworks appropriate to their security context. Organizations with such difficulties can be guided by this document in identifying and procuring appropriately competent services to assist.

The guidelines contained in this document do not provide detailed procedures at the technical or operational level. Where standards are not available at this level, organizations should formulate and implement procedures based on the high-level guidance contained in this document and according to best practices at international and national levels.

Security and resilience — Protective security — Guidelines for an enterprise protective security architecture and framework

1 Scope

This document provides guidance on the enterprise protective security architecture and the framework of protective security policies, processes and types of controls necessary to mitigate and manage security risks across the protective security domains, including:

a) security governance;

b) personnel security;

c) information security;

d) cybersecurity;

e) physical security.

This document is applicable for any organization.

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 22300, *Security and resilience — Vocabulary*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO 22300 and the following apply.

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

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

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

3.1
asset owner
person within the organization who is responsible for a given asset

3.2
business impact
impact on an organization's or sector's ability to operate resulting from the compromise of confidentiality, integrity or availability of assets

3.3
culture
shared values and attitudes that are applied within an organization by its personnel and interested parties

Note 1 to entry: This recognizes that an organization has a culture that, to varying degrees, supports and accepts security as part of business as usual; and that fostering this element of the organization's culture should be the aim of top management in delivering protective security outcomes.

3.4
cybersecurity
protection of the confidentiality, integrity, and availability of digital systems (hardware, software and associated infrastructure) from unauthorized digital access, harm or misuse, or attack scenarios that involve deliberate exploitation of computer systems, digitally-dependent enterprise networks and control systems

Note 1 to entry: This relates to a range of technical *domains* (3.5), including but not necessarily limited to *information and communications technology (ICT)* (3.9) and operational technology (OT).

3.5
domain
defined sphere of *protective security* (3.17) activity or knowledge

3.6
enterprise protective security architecture
documented structure comprising governance arrangements and the security framework elements by which protective security functions are performed and strategically aligned with the aims of the organization

3.7
framework
structure of policies, processes and specifications designed to support the accomplishment of an objective

Note 1 to entry: In this connection, a protective security framework consists of and aligns all elements of protective security policy and processes, including security *governance* (3.8), *personnel security* (3.15), *information security* (3.12), *cybersecurity* (3.4) and *physical security* (3.16).

3.8
governance
system of directing and controlling

Note 1 to entry: The processes by which organizations are directed, controlled and held to account, encompassing authority, accountability, stewardship, leadership, direction and control exercised in the organization.

3.9
information and communications technology
ICT
technology for gathering, storing, retrieving, processing, analysing and transmitting information

[SOURCE: ISO/IEC 30071-1:2019, 3.2.5]

3.10
information asset
knowledge or data that have value for the individual or organization (including intellectual property), which are defined and managed so it can be understood, shared, protected and used

3.11
information life cycle
process whereby information is managed over time, from the point of creation, receipt, distribution, use, maintenance and final disposal (disposition, destruction or archiving) according to the business impact of reduction or loss of the confidentiality, integrity or availability of information

3.12
information security
protection and preservation of the confidentiality, integrity and availability of all *information assets* (3.10), including information in transit (e.g. transactional security), digital security and *cybersecurity* (3.4)

Note 1 to entry: Information security relates to the security of information in all its forms (including hard copy and verbal communications), digital systems, *information and communications technology (ICT)* (3.10) and *operational technology (OT)*.

Note 2 to entry: Additional properties, such as authenticity, accountability, non-repudiation and reliability, can be included.

[SOURCE: ISO/IEC 27000:2018, 3.28, modified — definition has been extended and note 1 to entry has been added.]

3.13
measure
action or means to eliminate hazards or reduce risks

[SOURCE: ISO/IEC Guide 51:2014, 3.13, modified — example has been removed]

3.14
need-to-know
need to access specific information based on a business or operational requirement according to an active process of determining the security level of information and who has the right to access the information

3.15
personnel security
process of gaining and maintaining assurance of a person's eligibility and suitability (honesty, trustworthiness, maturity, resilience, loyalty and security competence) to access organizational assets

3.16
physical security
combination of physical *security controls* (3.19) to reduce the risk of unauthorized access, to safeguard assets and to protect from a potential security incident

3.17
protective security
processes and activities that protect assets from malicious acts, the impact of unintentional incidents and other events that can cause harm

Note 1 to entry: Protective security includes the following domains: security *governance* (3.8), *personnel security* (3.15), *information security* (3.12), *cybersecurity* (3.4) and *physical security* (3.16).

3.18
responsible security executive
RSE
person assigned within the organization's top management as the single point of responsibility for managing the organization's *security risk* (3.21)

Note 1 to entry: Having responsibility for managing the organization's security risk, the RSE is accountable to top management for the performance of that task. Top management is in turn accountable for the overall performance of the organization in general.

Note 2 to entry: The RSE is responsible for ensuring that the organization's security function is effectively managed and provides assurance to top management that security risks are being actively managed.

Note 3 to entry: Proper *governance* (3.8) requires that the RSE has the authority, resources and competence necessary to exercise this responsibility; and is part of, or has effective access to, top management.

3.19
security control
policy, process, or tangible or intangible risk reduction application which, on the basis of assessment, is implemented to treat risk by reducing or maintaining the likelihood of a security-related risk being realised, within specific levels or ranges

Note 1 to entry: This includes but is not limited to digital and physical access controls, alarms, active and passive surveillance, vetting and other personnel assessment tools.

Note 2 to entry: A security treatment is the actual application or implementation of one or more security controls to achieve an acceptable level of risk.

3.20
security in depth
defence in depth
protection in depth
use of multiple protective *security controls* (3.19) in layers across the enterprise to protect assets

Note 1 to entry: This recognizes that the strength of any system is no greater than its weakest link and ensures that if one control element fails, other defensive *measures* (3.13) are in place to continue providing protection.

3.21
security risk
potential that malicious actors (or any unintentional action or event) could harm or result in compromise, loss or unavailability of an organization's assets or reduce the effectiveness of *security controls* (3.19)

Note 1 to entry: See *security threat* 3.22.

Note 2 to entry: This definition draws on the definition of risk according to ISO 31000:2018, 3.1, in the context of security risk, where uncertainty in relation to the intent and capability of malicious actors and vulnerability to their actions can impact objectives.

3.22
security threat
threat that arises when the intentions and capabilities of malicious actors are committed to action and intersect with the vulnerabilities of protective *security controls* (3.19) or the intrinsic systems of an organization

Note 1 to entry: A vulnerability can be inherent in an asset or process or be caused by any event or circumstance, including a natural event or accident.

Note 2 to entry: Threat is sometimes considered as analogous to hazard (potential source of harm), although in the security context, hazard typically refers to materials or tools pre-existing in the operating environment that can be used by a malicious actor, such as explosives, malware, etc.

3.23
security vetting
processes designed to verify the identity of personnel and to provide assurance that they are eligible and suitable to access organizational assets

4 Enterprise protective security architecture

4.1 General

Protective security is optimized when it is aligned with protective security principles and led by the organization's top management. In that respect, the organization should implement governance arrangements that provide enterprise-level appreciation of security and deliver a framework of protective security policies, processes and specifications that are strategically aligned within the business.

4.2 Integration

Governance arrangements inform a security management programme which in turn should be incorporated within business operations in order to achieve the organization's security objectives.

The enterprise protective security architecture outlined in this document consists of the principles, governance arrangements and structural elements within which the framework of protective security policies, processes and specifications are implemented and managed.

Organizing security management along these lines requires support throughout the entire organization and strong leadership from top management and asset owners in particular. Also, since effective security risk management is key to security outcomes, the organization should undertake risk processes consistent with ISO 31000:2018, Clause 6 and ensure that all elements of security governance operate consistently with ISO 31000 in general.

Organizations should identify specific technical standards according to the need or, if these are not available, formulate and implement procedures based on the guidance contained in this document and according to best international and national practice.

Controls not directly related to security, but which can mitigate or accentuate security risk (emergency management and response, business continuity, crisis management, safety and privacy for example), should also be aligned within this enterprise protective security architecture.

4.3 Elements of the architecture

The organization should implement an enterprise protective security architecture consisting of the elements specified in Table 1.

Table 1 — Elements of the enterprise protective security architecture

Level		**Description**
1	Governance level: Protective security principles	The principles that drive strategy, objectives, resourcing and review of protective security at the organizational leadership and governance level.
2	Management level: Protective security domains	The domains of security practice that achieve these guiding principles in terms of the security of the organization's assets.
3	Implementation, operations and review level: Security risk management	The management of security risks enabling delivery of the objectives of the organization. Controls are implemented to mitigate/modify/treat security risk in relation to each of the security domains: security governance, personnel security, information security, cybersecurity, and physical security. A converged approach ensures that application of controls is complementary to the required security outcomes. Processes for measuring performance and for continuous improvement are included at this level.
	NOTE Monitoring performance is expanded upon in 6.2.2.7 and 6.2.2.8 and Clause 11.	

Elements of the enterprise protective security architecture can be expanded to align with the more detailed framework of organizational arrangements for security as outlined in Figure 1. Relevant technical standards can also assist in applying risk treatments. If these are not available, the organization should formulate and implement procedures based on this document.