ISO/FDIS 22342:~~2022~~2023(E)

Date: ~~2022-11-23~~2023-01-17

ISO/TC 292

Secretariat: SIS

Security and resilience — Protective security — Guidelines for the development of a security plan for an organization

ISO Copyright Office
CP 401 • CH-1214 Vernier, Geneva
Phone: + 41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org
Published in Switzerland.

Contents

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 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 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

All organizations seek to manage security risks in their environment to ensure appropriate protection levels of their assets, to preserve the interests of interested parties and to achieve their objectives.

Organizations sometimes need to establish and maintain a structured approach to security.

The purpose of a security plan is to ensure that all the appropriate actions and controls are in place to protect the organization from threats to its security.

This document ~~guides~~gives guidance on the implementation of a security plan whose structure includes the guidance for protective security architecture. Thus, the security plan can be effectively integrated into an existing management system.

Integrating the organization's risk management processes into the security plan model supports proper management of security. The security plan is designed to allocate accountability and responsibility, and to guide the application of controls to protect the organization from security risks.

A planned approach that is adaptive and agile makes it possible to provide solutions to unplanned situations. Security threats are dynamic and often unforeseen; therefore, this document introduces both technical and human-related elements for an adaptive and agile planned approach.

The intent of the document is to provide the fundamental elements necessary to improve and sustain the protection of an organization.

Security and resilience — Protective security — Guidelines for the development of a security plan for an organization

1 Scope

This document gives guidance on developing and maintaining security plans. ~~It is applicable to all organizations regardless of type, size and nature, whether in the private, public, or not-for-profit sectors, that wish to develop effective security plans in a consistent manner~~

The security plan describes how an organization establishes effective security planning and how it can integrate security within organizational risk management practices.

It is applicable to all organizations regardless of type, size and nature, whether in the private, public, or not-for-profit sectors, that wish to develop effective security plans in a consistent manner.

This document is applicable to any organization intending to implement measures designed to protect their assets against malicious acts and mitigate their associated risks.

This document does not provide specific criteria for identifying the need to implement or enhance prevention and protection measures against malicious acts. It does not apply to services and operations delivered by private security companies.

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~~:2021~~, *Security and resilience — Vocabulary*

ISO 31000~~:2018~~, *Risk management — Guidelines*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO 22300, ISO 31000 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
~~Need~~need-to-know
~~This expression means the~~ need to access specific information based on a business or operational requirement, involving an active process of determining the security level of information and who has the right to access the information~~.~~

4 Security planning

The organization should create, implement and maintain a security plan in order to manage activities based on security risk analysis and be aligned with the mission of the organization.

The security plan should:

— be specific to each organization;

— be based on security strategies and objectives regarding threats and vulnerabilities;

— be reviewed and formally endorsed by the top management board before implementation;

— foresee the need to face a long-term security-related incidents, incorporating special procedures, and the need for adaptive structures to be able to adequately deal with it such disruptive events.

The organization may use a single security plan or an overarching security plan supported by more detailed plans.

NOTE A single security plan is not always practical due to the organization's size or complexity of business.

5 Components of the security plan

5.1 General

This clause gives recommendations on how to develop the various components of a security plan. It consists of the following subclauses that give detailed guidance on:

— governance (see 5.2);

— management of risk (see 5.3);

— security controls (see 5.4);

— security controls process (see 5.5);.

NOTE ISO 28000:2022 clause, 8.6, also includes information regarding the content of a security plan.

5.2 Governance

5.2.1 General

The organization should determine how the security plan should be governed. This includes considering:

— Securitysecurity objectives (see 5.2.2);

— Scopescope of the security plan (See see 5.2.3);

— Leadership leadership (Seesee 5.2.4);

— Legallegal and regulatory (see 5.2.5);

— Rolesroles, accountabilities, and responsibilities (see 05.2.6);

— Communicationcommunication (see 5.2.7);

— ~~Documented~~documented information (see 5.2.8);

— ~~Reporting~~reporting (see 5.2.9);

— ~~Evaluation~~evaluation (see 5.2.10);

~~Continuous~~— continuous improvement (see 5.2.11).

5.2.2 Security objectives

The organization should define security objectives for the security plan that consider:

— broader business objectives and priorities;

— protective security framework;

— related security policies;

— security risk.

5.2.3 Scope of the security plan

The organization should determine the boundaries and applicability of the security plan to establish its scope.

This includes deciding if the security plan applies to all or part of the organization or if it just applies to a specific duration of a project.

The scope of the security plan should take into account any other organizational risk management process relevant to security threats or security violations.

The scope of the security plan should consider several criteria, including:

— missions and specificities of the organization's operations;

— external and internal issues;

— personnel concerned (including external personnel);

— tangible and intangible assets to be protected;

— places and spaces of the organization;

— places of travel or activities outside organizational facilities (if necessary);

— activities according to their nature and their relation to security aspects;

— any other relevant criteria.

In addition, the security plan should mention any applicable exclusions. The scope of the security plan should be available on a need-to-know basis.

5.2.4 Leadership

Top management should:

— specify the accountable leadership for the security plan and its management~~. This includes~~, including assigning the responsibility for creating, maintaining and executing the security plan to the organization security function, and holding assignees accountable for their performance;

— ensure the security plan includes guidance that ~~they receive~~top management receives appropriate reporting and reviews of the security status of the organization, and that actions for improvement are undertaken in response to such reviews;

— coordinate with asset owners and relevant security management personnel when developing the security plan to ensure that it supports the overall objectives of the organization;

— also communicate its commitment to security to the rest of the organization to promote a shared sense of community on the importance of security;

— provide the resources needed to implement the security plan.

5.2.5 Legal and regulatory

The organization should identify any applicable legal, regulatory and contractual obligations. This should also be taken into account when implementing the security plan. The organization should be in close contact with the authorities and communicate to them the responsibilities, provisions, and other key elements.

5.2.6 Roles, accountabilities and responsibilities

The organization should define and document security roles, responsibilities, and authorities for executing the security plan. This includes specifying:

— requisite skills for executing the plan;

— an assigned and defined level of competence for each role;

— the relationship between the internal security team and the external interested parties.

The security plan should align the security governance arrangements to general organizational governance. Where applicable, relationships with external security authorities that have governance roles should be defined. Exemptions to predefined security provisions should be listed, documented and reviewed.

5.2.7 Communication

The organization should communicate the contents and obligations of the security plan to relevant interested parties, including:

— top management's internal and external trusted relationships to share strategic information, best practices and lessons learned;

— responses to security emergencies and crises;

— roles and responsibilities.

The organization should also develop a policy for sharing information about its security and the application of "need-to-know".

