INTERNATIONAL STANDARD

ISO 22342

First edition
2023-04

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

Sécurité et résilience — Sûreté préventive — Lignes directrices pour l'élaboration d'un plan de sûreté destiné à un organisme

Reference number
ISO 22342:2023(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) 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

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

This document 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, *Security and resilience — Vocabulary*

ISO 31000, *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-to-know
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 in order to 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 long-term security-related incidents, while incorporating special procedures, and additionally should foresee the need for adaptive structures to be able to adequately deal with such disruptive events.

The organization may use a single security plan or a comprehensive and 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, 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:

— security objectives (see 5.2.2);

— scope of the security plan (see 5.2.3);

— leadership (see 5.2.4);

— legal and regulatory (see 5.2.5);

— roles, accountabilities and responsibilities (see 5.2.6);

— communication (see 5.2.7);

— documented information (see 5.2.8);

— reporting (see 5.2.9);

— evaluation (see 5.2.10);

— 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, 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 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".

5.2.8 Documented information

The organization should document the information necessary for the effectiveness of the plan, including:

— the scope of the security plan;

— past decisions regarding security risks (including shared and residual risks), treatments applied and their effectiveness;

— lessons learned from past decisions to enable the organization to take relevant actions for continuous improvement;

— policies and procedures that are relevant to the security plan.

5.2.9 Reporting

The security plan should include guidance to ensure top management receive appropriate reports concerning its execution.

5.2.10 Evaluation

The evaluation of the security plan should consider:

— the organization's approach to managing risk;

— security and strategic objectives;

— the resources needed, including staffing, training needs and required level of competence;

— results of the evaluation.

The organization should evaluate the effectiveness of the security plan based on:

— what needs to be evaluated;

— what methods to use for the evaluation;

— how the evaluation should be performed, analysed and reported;

— the defined frequency of the evaluations (e.g. normal and emergency situations);

— who is authorized to evaluate the security plan.

5.2.11 Continuous improvement

The organization should continually improve the security plan:

— actively seeking opportunities for improvement, even if not prompted by vulnerabilities related to security and imminent security threats or ongoing security violations;

— taking into consideration:

  — adjustments to the plan including risks and controls;

  — available resources for the plan including staffing, equipment and facilities.

5.3 Management of risk

5.3.1 General

Addressing risks to enable the security plan to achieve its intended results calls for an approach based on risk management that is customized for the organization. The interaction with the organization's overall planning should be acknowledged and aligned.

Depending on the level of risk to the assets to be protected, the required levels of protection should be defined for the assets, and controls implemented as determined to achieve the agreed level of acceptable risk.

The organization should manage its security risk by following the risk management process outlined in ISO 31000:2018, Clause 6, including:

— security risk scope, context and criteria (see 5.3.2);

— assessment (see 5.3.3);

— treatment (see 5.3.4);

— acceptance level for residual security risk (see 5.3.5);

— communication and consultation (see 5.3.6);

— monitoring and review (see 5.3.7);

— documentation management (see 5.3.8).

5.3.2 Security risk scope, context and criteria

When establishing the security plan, the organization should consider the external and internal security risk context relevant to its purpose and affecting its ability to achieve the intended results on a strategic level. This may include describing:

— tangible and intangible assets;

— asset value and the respective vulnerabilities requiring treatment;

— sources of security risks;

— partners and interested parties;

— globally significant trends;

— geographic or geopolitical considerations;

— the legal and regulatory environment;

— other aspects of its operating environment.

5.3.3 Assessment

The assessment of security risk should be done in accordance with ISO 31000:2018, Clause 6, which includes the following iterative process:

— risk identification;

— risk analysis;

— risk evaluation.

The security risk assessment process should be an integral part of management and integrated into the structure, operations and processes of the organization. It should be part of all organizational activities.

5.3.4 Treatment

The purpose of the treatment of security risk is to select and implement controls to mitigate risk. Treatment of security risk can include:

— treatment decisions for the given risk (avoiding the risk, removing the risk source, transferring the risk, sharing the risk, changing the likelihood, changing the consequences, accepting the risk and, where appropriate, by an acceptable reduction in performance or in protection levels);

— relevant security controls to mitigate the risk;

— retaining the risk by informed decision;

— controls and assessments designed to ensure measures are adequate;

— graduated security measures depending on special circumstances, such as the national threat level (treatment may also include exemptions to regulatory environments);

— establishing formal agreements with local law enforcement and equivalent agencies to address security threat intelligence sharing and security incidents.

5.3.5 Acceptance level for residual security risk

The acceptance level of residual security risks should be defined to enable the organization to make decisions about which security controls to apply. Any acceptance level of residual security risks should be based on the amount and type of risk the organization is likely to accept.

5.3.6 Communication and consultation

The communication of, and consultation regarding, security risk should include the arrangements by which communication of security risks will occur with internal and external interested parties. This should include:

— the relevant security risk context;

— key risk variables, such as likelihood, consequence, criticality and vulnerability;

— controls;

— sources of information on risk.

5.3.7 Monitoring and review

The security risk monitoring and review should be planned (both ongoing and periodic), including:

— clearly defining responsibilities regarding reporting activities;

— maintaining the confidentiality, integrity and availability of these reports.

5.3.8 Documentation management and recording

The organization should ensure that the security plan and other security documentation is managed in accordance with security and document control policies and procedures. This includes:

— storage and protection;

— restriction of access from unauthorized disclosure;

— disposal of documents in a secure manner;

— maintaining the confidentiality, integrity and availability of the security plan.

5.4 Security controls

5.4.1 General

The organization should ensure that the security plan addresses security controls, including:

— levels of protection (see 5.4.2);

— procedures for security controls (see 5.4.3);

— operational level controls and treatments (see 5.4.4);

— contingency planning for low likelihood and unforeseen situations (see 5.4.5);

— timelines for security activities (see 5.4.6).

The organization should ensure that all security operations are adequately planned, both regarding maintenance (regularly scheduled tasks) and intervention (those carried out to control incidents). In addition, the organization should ensure that information concerning the security controls is protected.

5.4.2 Levels of protection

The organization should define levels of protection for people, tangible and intangible assets that are:

— appropriate to different operational environments;

— subject to selection criteria to determine the appropriate treatment of security risk;

— reflective of the consequence ratings in setting the levels of risk acceptance;

— adaptive and responsive to changes in the operational environment.

5.4.3 Procedures for security controls

The procedures for security controls, including security operations and measures, should consider:

— operational risks;

— specific security risks;

— sources of risk;

— process for determining, defining and implementing security controls.

5.4.4 Operational level controls and treatments

The organization should develop operational level controls and treatments for the security plan. This includes reference to relevant policies, procedures, instructions and other security plans, as well as the adaptive mechanisms that will enable timely response to unanticipated events.

Processes designed to manage uncertainty and ambiguity should be included. This includes risks and controls across the protective security domains. These take into account:

— security governance:
  — roles and responsibilities;
  — risk tolerance;
  — security risk management (including threat, vulnerability and criticality assessments);
  — security incidents;
  — security culture;
  — security awareness and training;
  — security monitoring;
  — reporting security maturity;
  — contracted service providers;
— personnel security:
  — personnel security provisions during recruitment;
  — security clearance maintenance plans that address risks identified during security vetting;
  — processes regarding positions of trust or sensitive positions;
  — contact reporting;
  — security clearance management throughout the entire period of employment;
  — ongoing security awareness and training;
  — managing the separation of personnel;
— information security:
  — classification and management arrangements for information holdings;