INTERNATIONAL STANDARD

ISO/IEC 27014

Second edition
2020-12

Corrected version
2022-04

Information security, cybersecurity and privacy protection — Governance of information security

Sécurité de l'information, cybersécurité et protection de la vie privée — Gouvernance de la sécurité de l'information

Reference number
ISO/IEC 27014:2020(E)

© ISO/IEC 2020

COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2020

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

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

© ISO/IEC 2020 – All rights reserved

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 (see www.iso.org/directives or www.iec.ch/members_experts/refdocs)

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 https://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. In the IEC, see www.iec.ch/understanding-standards.

This document was prepared by ITU-T as ITU-T X.1054 (04/2021) and drafted in accordance with its editorial rules, in collaboration with Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *Information security, cybersecurity and privacy protection.*

This second edition cancels and replaces the first edition (ISO/IEC 27014:2013), which has been technically revised. The main changes compared to the previous edition are as follows:

— the document has been aligned with ISO/IEC 27001:2013;

— the requirements in ISO/IEC 27001 which are governance activities have been explained;

— the objectives and processes of information security governance have been described.

This corrected version of ISO/IEC 27014:2020 incorporates the following corrections:

— the document has been editorially revised in accordance with the rules-for-presentation-ITU-T-ISO-IEC common text.

© ISO/IEC 2020 – All rights reserved

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 and www.iec.ch/national-committees.

 © ISO/IEC 2020 – All rights reserved

INTERNATIONAL STANDARD ISO/IEC 27014
RECOMMENDATION ITU-T X.1054

Information security, cybersecurity and privacy protection – Governance of information security

Summary

Recommendation ITU-T X.1054 | International Standard ISO/IEC 27014 provides guidance on the governance of information security.

Information security is a key issue for organizations, amplified by rapid advances in attack methodologies and technologies, and corresponding increased regulatory pressures.

The failure of an organization's information security controls can have many adverse impacts on an organization and its interested parties including but not limited to the undermining of trust.

Governance of information security is the use of resources to ensure effective implementation of information security, and provides assurance that:

- directives concerning information security will be followed; and
- the governing body will receive reliable and relevant reporting about information security related activities.

This assists the governing body to make decisions concerning the strategic objectives for the organization by providing information about information security that may affect these objectives. It also ensures that information security strategy aligns with the overall objectives of the entity.

Managers and others working in organizations need to understand:

- the governance requirements that affect their work; and
- how to meet governance requirements that require them to take action.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T X.1054	2012-09-07	17	11.1002/1000/11594
2.0	ITU-T X.1054	2021-04-30	17	11.1002/1000/14248

Keywords

Information security, information security governance, information security management, ISMS.

* To access the Recommendation, type the URL http://handle.itu.int/ in the address field of your web browser, followed by the Recommendation's unique ID. For example, http://handle.itu.int/11.1002/1000/11830-en.

© ISO/IEC 2020 – All rights reserved

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents/software copyrights, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the appropriate ITU-T databases available via the ITU-T website at http://www.itu.int/ITU-T/ipr/.

© ITU 2022

All rights reserved. No part of this publication may be reproduced, by any means whatsoever, without the prior written permission of ITU.

© ISO/IEC 2020 – All rights reserved

CONTENTS

© ISO/IEC 2020 – All rights reserved

Introduction

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications. The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating, and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a world-wide basis. The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups that, in turn, produce Recommendations on these topics. The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1. In some areas of information technology that fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

ISO (the International Organization for Standardization) and IEC (the International Electro technical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of Recommendation | 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. In the field of Information security, cybersecurity and privacy protection, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

This Recommendation | International Standard has been drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare this Recommendation | International Standard. Draft Recommendation | International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75% of the national bodies casting a vote.

Attention is drawn to the possibility that some of the elements of this Recommendation | International Standard may be the subject of patent rights. ITU, ISO or IEC shall not be held responsible for identifying any or all such patent rights.

Rec. ITU-T X.1054 | ISO/IEC 27014 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *Information security, cybersecurity and privacy protection*, in collaboration with ITU-T SG17.

© ISO/IEC 2020 – All rights reserved

INTERNATIONAL STANDARD
ITU-T RECOMMENDATION

Information Security, Cybersecurity and Privacy Protection – Governance of Information Security

1 Scope

This Recommendation | International Standard provides guidance on concepts, objectives and processes for the governance of information security, by which organizations can evaluate, direct, monitor and communicate the information security-related processes within the organization.

The intended audience for this document is:

- governing body and top management;
- those who are responsible for evaluating, directing and monitoring an information security management system (ISMS) based on ISO/IEC 27001;
- those responsible for information security management that takes place outside the scope of an ISMS based on ISO/IEC 27001, but within the scope of governance.

This Recommendation | International Standard is applicable to all types and sizes of organizations.

All references to an ISMS in this document apply to an ISMS based on ISO/IEC 27001.

This Recommendation | International Standard focuses on the three types of ISMS organizations given in Annex B. However, it can also be used by other types of organizations.

2 Normative references

The following Recommendations and International Standards contain provisions which, through reference in this text, constitute provisions of this Recommendation | International Standard. At the time of publication, the editions indicated were valid. All Recommendations and Standards are subject to revision, and parties to agreements based on this Recommendation | International Standard are encouraged to investigate the possibility of applying the most recent edition of the Recommendations and Standards listed below. Members of IEC and ISO maintain registers of currently valid International Standards. The Telecommunication Standardization Bureau of the ITU maintains a list of currently valid ITU-T Recommendations.

– ISO/IEC 27000:in force, *Information technology – Security techniques – Information security management systems – Overview and vocabulary*.

– ISO/IEC 27001:in force, *Information technology – Security techniques – Information security management systems – Requirements*.

3 Definitions

For the purposes of this Recommendation | International Standard, the terms and definitions given in ISO/IEC 27000, and the following apply.

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

- IEC Electropedia: available at http://www.electropedia.org/
- ISO Online browsing platform: available at http://www.iso.org/obp
- ITU Terms and Definitions: available at http://www.itu.int/go/terminology-database

3.1 **entity**: Organization (3.2) and other bodies or parties.

NOTE – An entity can be a group of companies, or a single company, or a non for profit company, or other. The entity has governance authority over the organization. The entity can be identical to the organization, for example in smaller companies.

3.2 **organization**: That part of an entity (3.1) which runs and manages an ISMS.

3.3 **governing body**: Person or group of people who are accountable for the performance and conformance of the entity.

NOTE – SOURCE: ISO/IEC 27000:2018, 3.24, modified – "organization" has been replaced by "entity".

© ISO/IEC 2020 – All rights reserved

3.4 top management: Person or group of people who directs and controls an organization (3.2) at the highest level.

NOTE 1 – Source ISO/IEC 9001.

NOTE 2 – Top management has the power to delegate authority and provide resources within the organization.

NOTE 3 – If the scope of the management system covers only part of an entity, then top management refers to those who direct and control that part of the entity. In this situation, top management are accountable to the governing body of the entity.

NOTE 4 – Depending on the size and resources of the organization, top management can be the same as the governing body.

NOTE 5 – Top management reports to the governing body. [SOURCE: ISO/IEC 27000:2018, 3.75].

NOTE 6 – ISO/IEC 37001 also provides definitions for governing body and top management.

4 Abbreviations

For the purposes of this Recommendation | International Standard, the following abbreviations apply:

ISMS Information Security Management System

IT Information Technology

5 Use and structure of this Recommendation | International Standard

This Recommendation | International Standard describes how information security governance operates within an ISMS based upon ISO/IEC 27001, and how these activities can relate to other governance activities which operate outside the scope of an ISMS. It outlines four main processes of "evaluate", "direct", "monitor" and "communicate" in which an ISMS can be structured inside an organization, and suggests approaches for integrating information security governance into organizational governance activities in each of these processes. Finally, Annex A describes the relationships between organizational governance, governance of information technology and governance of information security.

The ISMS covers the whole of the organization, by definition (see ISO/IEC 27000). It can cover the whole of the entity, or part of the entity. This is illustrated in Figure B.1.

6 Governance and management standards

6.1 Overview

Governance of information security is the means by which an organization's governing body provides overall direction and control of activities that affect the security of an organization's information. This direction and control focuses on circumstances where inadequate information security can adversely affect the organization's ability to achieve its overall objectives. It is common for a governing body to realise its governance objectives by:

- providing direction by setting strategies and policies;
- monitoring the performance of the organization; and
- evaluating proposals and plans developed by managers.

Management of information security is associated with ensuring the achievement of the objectives of the organization described within the strategies and policies established by the governing body. This can include interacting with the governing body by:

- providing proposals and plans for consideration by the governing body; and
- providing information to the governing body concerning the performance of the organization.

Effective governance of information security requires both members of the governing body and managers to fulfil their respective roles in a consistent way.

6.2 Governance activities within the scope of an ISMS

ISO/IEC 27001 specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system within the context of an organization. It also includes requirements for the assessment and treatment of information security risks tailored to the needs of the organization.

ISO/IEC 27001 does not use the term "governance" but specifies a number of requirements which are governance activities. The following list provides examples of these activities. References to the organization and top management are, as previously noted, associated with the scope of an ISMS based on ISO/IEC 27001.

© ISO/IEC 2020 – All rights reserved

- ISO/IEC 27001:2013, 4.1 requires the organization to identify what it is aiming to achieve – its information security goals and objectives. These should be related to, and support, the overall goals and objectives of the entity. This relates to governance objectives 1, 3 and 4 stated in 7.2 of this Recommendation | International Standard.
- ISO/IEC 27001:2013, 4.2 requires the organization to identify the interested parties that are relevant to its ISMS, and the requirements of those interested parties relevant to information security. This relates to governance objective 4 stated in 7.2 of this Recommendation | International Standard.
- ISO/IEC 27001:2013, 4.3 requires the organization to define the boundaries and applicability of the ISMS to establish its scope by considering the external issues and internal issues, the requirements, and interfaces and dependencies. It is also specified that the organization shall build the requirements and expectations of interested parties into its information security management system, as well as external and internal issues (such as laws, regulations and contracts). This relates to governance objective 1 stated in 7.2 of this Recommendation | International Standard.
- ISO/IEC 27001:2013, 5 specifies that the organization shall set policy, objectives, and integrate information security into its processes (which can be considered to include governance processes). It requires the organization to make suitable resources available and communicate the importance of information security management. Most importantly, it also states that the organization shall direct and support persons to contribute to the effectiveness of the ISMS, and that other relevant management roles shall be supported in their areas of responsibility. ISO/IEC 27001:2013, 5 contains instructions for setting policy, and assigning roles for information security management and reporting. This relates to governance objectives 1 and 3 stated in 7.2 of this Recommendation | International Standard.
- ISO/IEC 27001:2013, 6 considers the design of a risk management approach for the organization, specifying that the organization shall identify risks and opportunities to be addressed to ensure that its ISMS is effective. It introduces the concept of risk owners, and puts their responsibilities into the context of the organization's activities to manage risk and approve risk treatment activities. It also requires the organization to establish information security objectives. This relates to governance objective 2 stated in 7.2 of this Recommendation | International Standard.
- ISO/IEC 27001:2013, 7 specifies that persons shall be competent in carrying out their information security obligations, and provides a requirement for organizational communications. This relates to governance objective 5 stated in 7.2 of this Recommendation | International Standard.
- ISO/IEC 27001:2013, 8 specifies the responsibility of the organization to plan, implement and control its ISMS, including outsourced arrangements. This relates to governance objectives 4 and 6 stated in 7.2 of this Recommendation | International Standard.
- ISO/IEC 27001:2013, 9 requires monitoring and reporting of all relevant aspects of the ISMS, internal audits, and top management and governing body review and decisions on the operational effectiveness of the ISMS, including any changes required. This relates to governance objective 6 stated in 7.2 of this Recommendation | International Standard.
- ISO/IEC 27001:2013, 10 specifies the identification and treatment of non-conformities, the requirement for identification of opportunities for continual improvement, and acting on those opportunities. This relates to governance objective 4 stated in 7.2 of this Recommendation | International Standard.

6.3 Other related standards

ISO/IEC 38500 provides guiding principles for members of governing bodies of organizations on the effective, efficient, and acceptable use of information technology within their organizations. It also provides guidance to those advising, informing, or assisting governing bodies in governance of IT.

6.4 Thread of governance within the organization

These threads are in exact correspondence to the organizational governance processes described in 7. The last two items in the list are equivalents of their governance aspects in the context of information security:

- the alignment of the information security objectives with the business objectives;
- the management of information security risk in accordance with those information security objectives;
- the avoidance of conflicts of interest in the management of information security;
- preventing the organization's information technology from being used to harm other organizations.

© ISO/IEC 2020 – All rights reserved

7 Entity governance and information security governance

7.1 Overview

There are many areas of governance within an entity, including information security, information technology, health and safety, quality and finance. Each governance area is a component of the overall governance objectives of an entity, and thus should be aligned with the discipline of the entity. The scopes of governance models sometimes overlap. Clauses 7.2 and 7.3 describe objectives and processes involved in information security governance, which can apply to any area being governed.

An ISMS focuses on management of risks relating to information. It does not directly address subjects such as profitability, acquisition, use and realization of assets, or the efficiency of other processes, although it should support any organizational objectives on these subjects.

7.2 Objectives

7.2.1 Objective 1: Establish integrated comprehensive entity-wide information security

Governance of information security should ensure that information security objectives are comprehensive and integrated. Information security should be handled at an entity level, with decision making taking into account entity priorities. Activities concerning physical and logical security should be closely coordinated. This does not, however, require a single set of security measures, or a single information security management system (ISMS) across the entity.

To ensure entity-wide information security, responsibility and accountability for information security should be established across the full span of an entity's activities. This can extend beyond the generally perceived "borders" of an entity e.g., to include information being stored or transferred by external parties.

7.2.2 Objective 2: Make decisions using a risk-based approach

Governance of information security should be based on compliance obligations, and also on entity-specific risk-based decisions. Determining how much security is acceptable should be based on the risk appetite of an entity, including loss of competitive advantage, compliance and liability risks, operational disruptions, reputational harm, and financial loss.

Information security risk management should be consistent across the entity and include considerations of the adverse financial, operational, and reputational impacts of breaches and non- compliance. Furthermore, information security risk management should be integrated with the entity's overall risk management approach, so it is not done in isolation and does not cause confusion, for example, mapping to the entity methodology or capturing strategic information risks into the entity's risk register.

Appropriate resources to implement information risk management should be allocated as a part of the security governance process.

7.2.3 Objective 3: Set the direction of acquisition

The impact of information security risk should be adequately assessed when undertaking new activities, including but not limited to, any investment, purchases, merger, adoption of new technology, outsourcing arrangements and contract with external suppliers.

To optimize information security acquisition to support entity objectives, the governing body should ensure that information security is integrated with existing entity processes, including project management, procurement, financial expenditure, legal and regulatory compliance, and strategic risk management.

The top management for each ISMS should establish an information security strategy based on organizational objectives, ensuring harmonization between entity requirements and organizational information security requirements, thereby meeting the current and evolving needs of interested parties.

7.2.4 Objective 4: Ensure conformance with internal and external requirements

Governance of information security should ensure that information security policies and practices conform to requirements of interested parties. These can include legislation and regulations, as well as contractual requirements and internal commitments.

To address conformance and compliance issues, top management can obtain assurance that information security activities are satisfactorily meeting internal and external requirements by commissioning independent security audits.

© ISO/IEC 2020 – All rights reserved

7.2.5 Objective 5: Foster a security-positive culture

Governance of information security should be built on entity culture, including the evolving needs of all the interested parties, since human behaviour is one of the fundamental elements to support the appropriate level of information security. If not adequately coordinated, the objectives, roles, responsibilities and resources can conflict with each other, resulting in the failure to meet any objectives. Therefore, harmonization and concerted orientation between the various interested parties is very important.

To establish a positive information security culture, top management should require, promote and support coordination of interested party activities to achieve a coherent direction for information security. This supports the delivery of security education, training and awareness programs. Information security responsibilities should be integrated into the role of staff and other parties, and they should support the success of each ISMS by taking on these responsibilities.

7.2.6 Objective 6: Ensure the security performance meets current and future requirements of the entity

Governance of information security should ensure that the approach taken to protect information is fit for purpose in supporting the entity, providing agreed levels of information security. Security performance should be monitored and maintained at levels required to meet current and future requirements.

To review performance of information security from a governance perspective, the governing body should evaluate the performance of information security in relation to its entity level impact, not just the effectiveness and efficiency of security controls.

Within each ISMS, top management of ISMS should be required to implement a performance measurement program to monitor, audit, and identify opportunities for improvement. The governing body should link information security performance to the performance of the organization, and of the entity.

7.3 Processes

7.3.1 General

The governing body within an entity performs the "evaluate", "direct", "monitor" and "communicate" processes. Figure 1 shows the relationship between these processes.

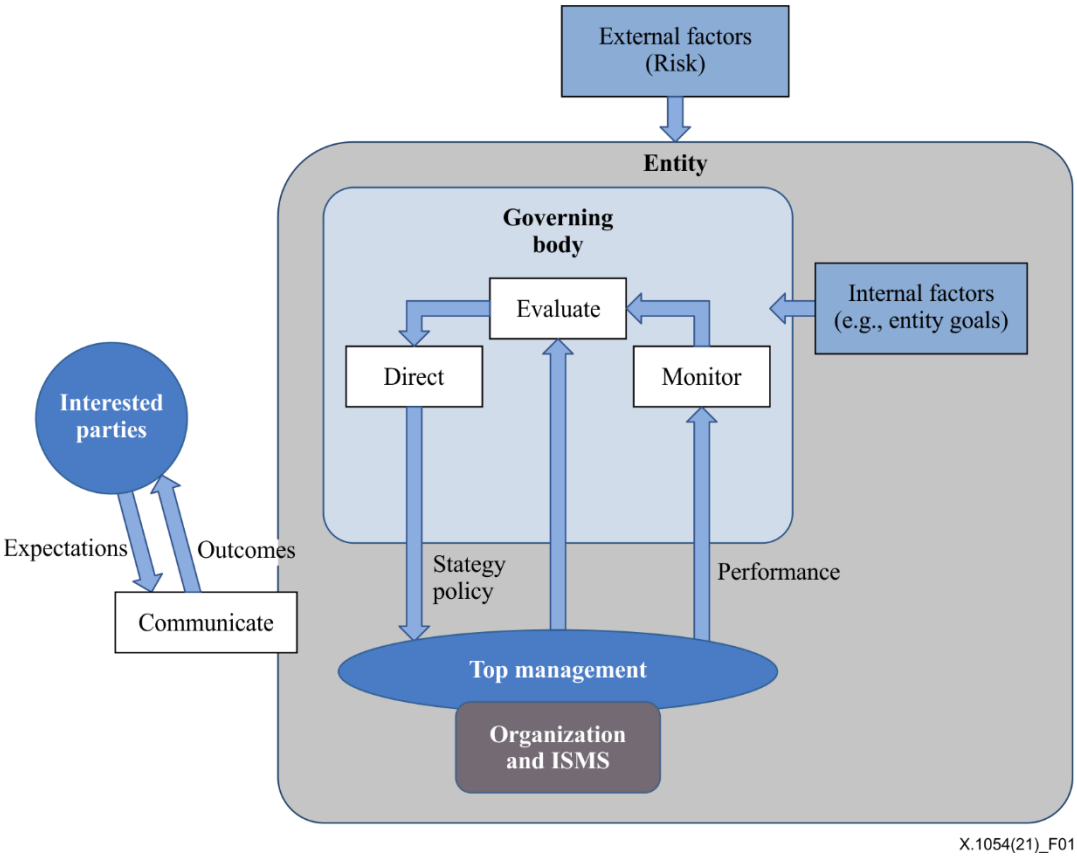

Figure 1 – Governance model for an entity with one ISMS

© ISO/IEC 2020 – All rights reserved

NOTE 1 – The definition of organization [3.2] means that top management is always fully involved in the operation of the organization.

NOTE 2 – An entity can contain more than one ISMS and there may be parts of an entity, to which governance applies, that are not part of an ISMS. See clause 8 and Annex B.

7.3.2 Evaluate

"Evaluate" is the governance process that considers the current and forecast achievement of objectives based on current processes and planned changes, and determines where any adjustments are required to optimize the achievement of strategic objectives in the future.

To perform the "evaluate" process:

- the governing body of the entity should:
  - ensure that initiatives take into account relevant risks and opportunities;
  - respond to information security and ISMS measurements and reports by specifying and prioritizing required objectives in the context of each ISMS (which includes consideration of the requirements from outside the ISMS scope); and
- the top management of each ISMS should:
  - ensure that information security adequately supports and sustains the entity's objectives;
  - submit new information security projects with significant impact to the governing body for approval.

7.3.3 Direct

"Direct" is the governance process by which the governing body gives direction about the entity's objectives and strategy. Direction can include changes in resourcing levels, allocation of resources, prioritization of activities, and approvals of policies, material risk acceptance and risk management plans.

To perform the "direct" process:

- the governing body should:
  - set the overall strategic direction and objectives of the entity;
  - define the entity's risk appetite;
  - approve the information security strategy; and
- the top management of each ISMS should:
  - allocate adequate investment and resources;
  - align organizational information security objectives with the entity's objectives;
  - allocate roles and responsibilities for information security;
  - establish an information security policy.

NOTE – Risk appetite is amount and type of risk that an organization is willing to pursue or retain. [8]

7.3.4 Monitor

"Monitor" is the governance process that enables the governing body to assess the achievement of strategic objectives.

To perform the "monitor" process:

- the governing body should:
  - receive the report on the effectiveness of the operation of each ISMS;
  - evaluate these in the context of the priorities of the entity;
  - communicate priorities to top management of each ISMS; and
- the top management of each ISMS should:
  - assess the effectiveness of information security management activities;
  - ensure conformance with internal and external requirements;
  - consider the changing entity, legal and regulatory environments, and any potential impact on information risk;
  - select appropriate performance metrics and require reporting to take place in a timely manner from an organizational perspective;

© ISO/IEC 2020 – All rights reserved

- provide feedback on information security performance results to the governing body;
- alert the governing body of new developments affecting information risks and information security.

To review performance of information security from a governance perspective, the top management should evaluate the performance of information security in relation to its impact at an organizational and entity level, not just the effectiveness and efficiency of security controls. This can be done by implementing a performance measurement program to monitor, audit, and identify opportunities for improvement, linking information security performance to the performance of the organization and of the entity.

7.3.5 Communicate

"Communicate" is the bi-directional governance process by which the governing body and interested parties exchange information appropriate to their specific needs.

A method which can be used to "communicate" is a statement of information security status which explains information security activities and issues to interested parties.

One of the reasons for communication is to allow entities to be held accountable to interested parties such as shareholders. This is becoming more important, and organizations now provide information on their implementation and maintenance of information security management, as well as its effectiveness in managing risk. Equally, in the case where an information security incident has taken place, entities should explain the impact, cause, and changes to controls to address risk of repeated incidents to their interested parties, and separately to the public as appropriate.

Communication can be carried out by a variety of methods. It can also have a variety of content. It also has a variety of audiences. Any communication should be designed to take the audience into account, as well as the message which it is intended that the audience should understand. These two factors should then be used to determine the content of the communications, as well as the channels used to deliver the communications to the intended audience. One example is shown in Annex C.

To perform the "communicate" process:

– the governing body should:
  - report to external interested parties that the entity practices a level of information security commensurate with the nature of its activities and priorities;
  - identify and prioritize regulatory obligations, interested parties' expectations, and the entity's requirements with regard to information security;
  - advise top management of each ISMS of any matters that require its attention and decision;
  - instruct relevant interested parties on detailed objectives to be taken in support of information security priorities;
  - promote a positive information security culture;
  - train and communicate with staff and other persons in scope of the ISMS on their responsibilities.

8 The governing body's requirements on the ISMS

8.1 Organization and ISMS

The governing body should require the design of one or more ISMSs to support the entity's objectives. The objectives of each ISMS can be the same as those of the parent entity or different, depending on the size, scale and structure of the entire entity, but they should be aligned. Possible relationships between governance of information security and governance of information technology are illustrated in Annex A.

The governing body should also require the design of each ISMS to be consistent with overall entity policies and processes, including risk management. It can be appropriate for an ISMS to adopt the same risk assessment process as that of the governing body, to enable clear communication of risk information. If the governing body uses a risk assessment process which does not conform to the requirements of ISO/IEC 27001, then, if the organization wishes to achieve compliance, its ISMS should use a different risk assessment approach to that used by the entity, and agree on a method for communicating risk related information to the governing body in terms which are compatible with the governing body's approach. Alternatively, the governing body can choose to alter the entity's existing risk assessment process to conform to the requirements of ISO/IEC 27001.

The governing body can mandate use of an ISMS to manage those strategic risks which relate to the loss of intellectual property, damage to reputation, and financial losses associated with damage to information's confidentiality, integrity or availability.

© ISO/IEC 2020 – All rights reserved

An ISMS can supply the governing body with management information relating to:

- risks to the entity;
- effectiveness of the ISMS.

The governing body should:

- approve the creation of each ISMS;
- define the scope of each ISMS and for certification (these scopes can differ);
- provide direction to each ISMS including objectives, requirements, roles and resources;
- make decisions on acceptable levels of residual risk, or appropriate risk treatments;
- provide each ISMS with communications channels and the authority to use those channels to communicate the appropriate information to interested parties and all persons in the scope of that ISMS.

8.2 Scenarios (see Annex B)

8.2.1 Type A: The ISMS organization is the whole entity

Where the only management system in place is conformant with ISO/IEC 27001, it can be used to supply risk information and thereby allow an organization to govern information risk. However, different processes still exist to support IT governance, financial governance, operational governance, and other governance activities.

In the case where the ISMS organization applies to the whole entity:

- The governance processes as described in 7.3 are unchanged;
- Top management has governance responsibilities in addition to information security governance, e.g., corporate governance.

Alignment of the organization's information security objectives with the entity's overall objectives is likely to be straightforward, since top management is responsible for setting both. If a single role holds responsibility for both governance and management of information security, adequate advice should be provided to ensure that accountability for setting of policy, and for its execution, are adequately separated from one another.

8.2.2 Type B: The ISMS organization forms a part of a larger entity

Some ISMS organizations form part of a larger entity. Since governance activities usually apply to a whole legal entity, corporation, charity, public body or other entity, the governance of that entity extends in this case beyond the scope of the ISMS. An organization can have multiple ISMSs within its boundaries. Thus, a governing body can govern multiple ISMSs. The majority of this document is written to allow for this approach.

The four governance processes as described in 7.3 remain relevant. However, depending on the relationship between the ISMS organization(s) and the parent entity, one of the following situations can apply.

- Each ISMS organization operates as an autonomous part of the parent entity and therefore has its own business objectives. In this case, the ISMS organization's information security objectives should be aligned with its own business objectives.
- Each ISMS organization is responsible for achieving one or more of its parent entity's business objectives. In this case, the ISMS organization's information security objectives should be aligned with its parent entity's business objectives.

Each ISMS organization has been assigned responsibility for managing an aspect of information security risk on behalf of the parent entity. In this case, the ISMS organization's information security objectives should be specified by the parent entity, which ensures alignment with the parent entity's business objectives.

There is also a relationship between the top management of each ISMS organization and the governing body of the parent entity. The top management team(s) and the governing body can be the same, can have some people in common or can have none in common. Figure B.1 should be used to determine which individuals should be assigned to the roles of governing body member and interested party.

8.2.3 Type C: The ISMS organization includes parts of several entities

In this situation, the ISMS organization is governed and controlled by top management as usual, but spans a number of entities. This can be seen in the case where a larger entity governs a group of entities which share a common information security context and requirements for a subset of their activities, for example where personal data is collected, processed, stored and used to provide services. Multiple governing bodies can also share one ISMS; for example, an organization can provide an ISMS as a service for use by many customers.

© ISO/IEC 2020 – All rights reserved

In the case where the ISMS organization includes parts of several entities,

- The governance processes as described in 7.3 are unchanged;
- The ISMS organization's information security objectives should be aligned with the mutual business objectives that bind the member entities together.

© ISO/IEC 2020 – All rights reserved

Annex A

Governance relationship

(This annex does not form an integral part of this Recommendation | International Standard.)

The relationship between governance of information security and governance of information technology is illustrated in Figure A.1.

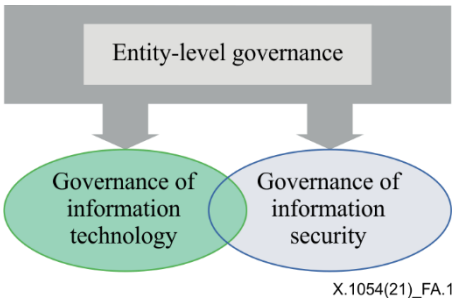

Figure A.1 – Relationship between governance of information security and governance of information technology

Whereas the overarching scope of governance of information technology aims at resources required to acquire, process, store and disseminate information, the scope of governance of information security covers confidentiality, integrity and availability of information. Both governance schemes can be handled by the following governance processes: evaluate, direct, monitor and communicate.

© ISO/IEC 2020 – All rights reserved

Annex B

Types of ISMS organization

(This annex does not form an integral part of this Recommendation | International Standard.)

There are three types of relationship between an organization which manages an ISMS, and an entity which applies an ISMS. These relationships also affect the membership of the top management of the ISMS and the governing body of the entity. The list below and Figure B.1 illustrate these types of relationship.

Type A: The entity and the ISMS organization are the same.

- The governing body is the same as the top management for the ISMS.

Type B: The entity contains the ISMS organization (and more than one ISMS may be in operation within that entity).

- The governing body can share some members with each ISMS, but the membership is not identical.

Type C: One ISMS is shared by multiple entities:

- If the entities have a direct interest in the ISMS, the governing body of each entity can have membership on the top management of the ISMS;
- If the ISMS is being provided as a service by a third party, membership of the top management of the ISMS is unlikely to include members of the governing bodies of the entities sharing the ISMS.

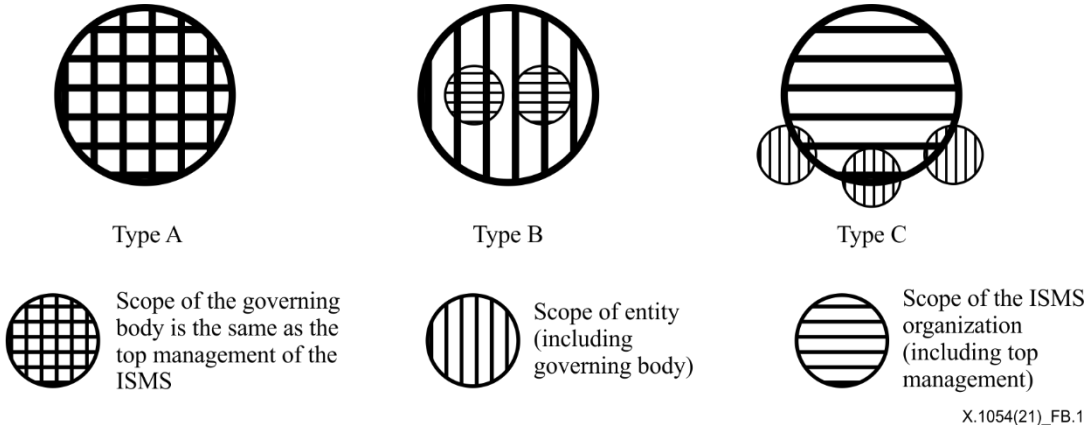

Figure B.1 – Possible relationships of an entity(ies) and its ISMS(es)

© ISO/IEC 2020 – All rights reserved

Annex C

Examples of communication

(This annex does not form an integral part of this Recommendation | International Standard.)

One example of communication is seen in stock markets where companies are obliged to disclose information security risks due to laws, or industry rules. Another example is an environmental, social and governance (ESG) report as a means for organizations to explain/communicate their efforts from environmental, social and economic perspectives to interested parties. Some ESG reports describe the approach to privacy data protection, information security activities and crisis management for prevention of security incidents.

Communications design activities should also consider the unintended effects of an audience misunderstanding or inferring additional content, and of the communications reaching persons other than the intended audience.

© ISO/IEC 2020 – All rights reserved

Bibliography

[1] Recommendation ITU-T X.1051 (2016) | ISO/IEC 27011:2016, *Information technology – Security techniques – Code of practice for Information security controls based on ISO/IEC 27002 for telecommunications organizations*.

[2] ISF, Standard of Good Practice for Information Security: 2018.

[3] ISO 37001:2016, *Anti-bribery management systems – Requirements with guidance for use*.

[4] ISO/IEC 9001:2015, *Quality management systems – Requirements*.

[5] ISO/IEC 27000:2018, *Information security, cybersecurity and privacy protection – Overview and vocabulary*.

[6] ISO/IEC 27002:2013, *Information security, cybersecurity and privacy protection – Code of practice for information security controls*.

[7] ISO/IEC 38500:2015, *Information technology – Governance of IT for the organization*.

[8] ISO Guide 73:2009

[9] IT Governance Institute (ITGI), *Information Security Governance: Guidance for Information Security Managers: 2008*.

[10] ITGI, *Information Security Governance Guidance for Boards of Directors and Executive Management*, 2nd Edition: 2006.

[11] ITGI, *COBIT Control Practices: Guidance to Achieve Control Objective for Successful IT Governance*, 2nd Edition: 2007.

[12] Ohki E., Harada Y., Kawaguchi S., Shiozaki T., Kgaua T., *Information Security Governance framework, Proceedings of the first ACM workshop on Information security governance*, pp. 1-6, 2009.

© ISO/IEC 2020 – All rights reserved

ICS 35.030

Price based on 13 pages

© ISO/IEC 2020 – All rights reserved