INTERNATIONAL STANDARD

ISO/IEC 27014

First edition
2013-05-15

Information technology — Security techniques — Governance of information security

Technologies de l'information — Techniques de sécurité — Gouvernance de la sécurité de l'information

Reference number
ISO/IEC 27014:2013(E)

COPYRIGHT PROTECTED DOCUMENT

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

CONTENTS

Page

Summary ..... **iv**

Foreword ..... **v**

1 Scope **1**

2 Normative references **1**

3 Definitions **1**

4 Concepts **2**
4.1 General **2**
4.2 Objectives **2**
4.3 Desired Outcomes **2**
4.4 Relationship **2**

5 Principles and processes **3**
5.1 Overview **3**
5.2 Principles **3**
5.3 Processes **5**
5.3.1 Overview **5**
5.3.2 Evaluate **5**
5.3.3 Direct **6**
5.3.4 Monitor **6**
5.3.5 Communicate **6**
5.3.6 Assure **7**

Annex A (informative) **An example of information security status** **8**

Annex B (informative) **An example of detailed information security status** **9**

Bibliography **11**

INTERNATIONAL STANDARD <ISO/IEC 27014>

ITU-T RECOMMENDATION <X.1054>

Information technology — Security techniques — Governance of information security

Summary

This Recommendation | International Standard provides guidance on the governance of information security.

Information security has become a key issue for organisations. Not only are there increasing regulatory requirements but also the failure of an organisation's information security measures can have a direct impact on an organisation's reputation.

Therefore, the governing body, as part of its governance responsibilities, is increasingly required to oversee information security to ensure the objectives of the organisation are achieved.

In addition, governance of information security provides a powerful link between an organisation's governing body, executive management and those responsible for implementing and operating an information security management system.

It provides the mandate essential for driving information security initiatives throughout the organisation.

Furthermore, an effective governance of information security ensures that the governing body receives relevant reporting - framed in a business context - about information security-related activities. This enables pertinent and timely decisions about information security issues in support of the strategic objectives of the organisation.

Foreword

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 Organisation 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 International Standards through technical committees established by the respective organisation to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organisations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

International Standards are 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 International Standards. Draft 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 document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

ISO/IEC 27014 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*, in collaboration with ITU-T. The identical text is published as ITU-T Recommendation X.1054.

1 Scope

This Recommendation | International Standard provides guidance on concepts and principles for the governance of information security, by which organisations can evaluate, direct, monitor and communicate the information security related activities within the organisation.

This International Standard is applicable to all types and sizes of organisations.

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 27000:2009, *Information Technology – Security techniques – Information security management systems – Overview and vocabulary*

3 Definitions

For the purposes of this Recommendation | International Standard, the terms and definitions in ISO/IEC 27000:2009 and the following definitions apply:

3.1
executive management
person or group of people who have delegated responsibility from the governing body for implementation of strategies and policies to accomplish the purpose of the organisation.

NOTE 1 Executive management form part of top management: For clarity of roles, this standard distinguishes between two groups within top management: the governing body and executive management.

NOTE 2 Executive management can include Chief Executive Officers (CEOs), Heads of Government Organizations, Chief Financial Officers (CFOs), Chief Operating Officers (COOs), Chief Information Officers (CIOs), Chief Information Security Officers (CISOs), and like roles.

3.2
governing body
person or group of people who are accountable for the performance and conformance of the organisation

NOTE Governing body forms part of top management: For clarity of roles, this standard distinguishes between two groups within top management: the governing body and executive management.

3.3
governance of information security
system by which an organisation's information security activities are directed and controlled

3.4
stakeholder
any person or organisation that can affect, be affected by, or perceive themselves to be affected by an activity of the organisation.

NOTE A decision maker can be a stakeholder.

4 Concepts

4.1 General

Governance of information security needs to align objectives and strategies for information security with business objectives and strategies, and requires compliance with legislation, regulations and contracts. It should be assessed, analysed and implemented through a risk management approach, supported by an internal control system.

The governing body is ultimately accountable for an organisation's decisions and the performance of the organisation. In respect to information security, the key focus of the governing body is to ensure that the organisation's approach to information security is efficient, effective, acceptable and in line with business objectives and strategies giving due regard to stakeholder expectations. Various stakeholders can have different values and needs.

4.2 Objectives

The objectives of governance of information security are to:

- align the information security objectives and strategy with business objectives and strategy (strategic alignment)
- deliver value to the governing body and to stakeholders (value delivery)
- ensure that information risk is being adequately addressed (accountability)

4.3 Desired Outcomes

The desired outcomes from effectively implementing governance of information security include:

- governing body visibility on the information security status
- an agile approach to decision-making about information risks
- efficient and effective investments on information security
- compliance with external requirements (legal, regulatory or contractual)

4.4 Relationship

There are several other areas of governance models within an organisation, such as governance of information technology, and organisational governance. Every governance model is an integral component of the governance of an organisation, which emphasizes the importance of alignment with business objectives. It is usually beneficial for the governing body to develop a holistic and integrated view of its governance model, of which governance of information security should be a part. The scopes of governance models sometimes overlap. For example, the relationship between governance of information security and governance of information technology is illustrated in Figure 1.

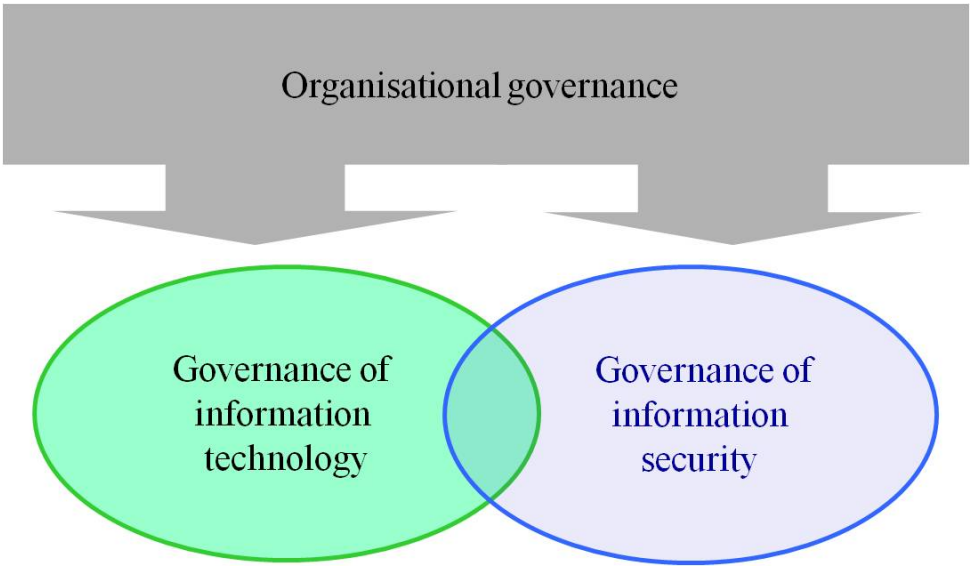

Figure 1 — Relationship between governance of information security and governance of information technology

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 need to be handled by the following governance processes: EDM (Evaluate, Direct, Monitor). However the governance of information security requires the additional internal process "communicate".

The tasks required of the governing body to establish governance of information security are described in Clause 5. Governance tasks are also related to management requirements specified in ISO/IEC 27001 as well as to other standards of the ISMS family, as referenced in the Bibliography.

5 Principles and processes

5.1 Overview

This clause describes the principles and processes that, together, form the governance of information security. Governance principles of information security are accepted rules for governance action or conduct that act as a guide for the implementation of governance. A governance process for information security describes a series of tasks enabling the governance of information security and their interrelationships. It also shows a relationship between governance and the management of information security. These two components are explained in the following subclauses.

5.2 Principles

Meeting the needs of stakeholders and delivering value to each of them is integral to the success of information security in the long term. To achieve the governance objective of aligning information security closely with the goals of the business and to deliver value to stakeholders, this sub-clause sets out six action-oriented principles.

The principles provide a good foundation for the implementation of governance processes for information security. The statement of each principle refers to what should happen, but does not prescribe how, when or by whom the principles would be implemented because these aspects are dependent on the nature of the organisation implementing the principles. The governing body should require that these principles be applied and appoint someone with responsibility, accountability, and authority to implement them.

Principle 1: Establish organisation-wide information security

Governance of information security should ensure that information security activities are comprehensive and integrated. Information security should be handled at an organisational level with decision-making taking into account business, information security, and all other relevant aspects. Activities concerning physical and logical security should be closely coordinated.

To establish organisation-wide security, responsibility and accountability for information security should be established across the full span of an organisation's activities. This regularly extends beyond the generally perceived 'borders' of the organisation e.g. with information being stored or transferred by external parties.

Principle 2: Adopt a risk-based approach

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

To adopt an information risk management appropriate to the organisation, it should be consistent and integrated with the organisation's overall risk management approach. Acceptable levels of information security should be defined based upon the risk appetite of an organisation, including the loss of competitive advantage, compliance and liability risks, operational disruptions, reputational harm, and financial losses. Appropriate resources to implement information risk management should be allocated by the governing body.

Principle 3: Set the direction of investment decisions

Governance of information security should establish an information security investment strategy based on business outcomes achieved, resulting in harmonization between business and information security requirements, ‚both in short and long term„ thereby meeting the current and evolving needs of stakeholders.

To optimize information security investments to support organisational objectives, the governing body should ensure that information security is integrated with existing organisation processes for capital and operational expenditure, for legal and regulatory compliance, and for risk reporting.

Principle 4: Ensure conformance with internal and external requirements

Governance of information security should ensure that information security policies and practices conform to relevant mandatory legislation and regulations, as well as committed business or contractual requirements and other external or internal requirements.

To address conformance and compliance issues, the governing body should obtain assurance that information security activities are satisfactorily meeting internal and external requirements by commissioning independent security audits.

Principle 5: Foster a security-positive environment

Governance of information security should be built upon human behaviour, including the evolving needs of all the stakeholders, 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 may conflict with each other, resulting in the failure to meet business objectives. Therefore, harmonization and concerted orientation between the various stakeholders is very important.

To establish a positive information security culture, the governing body should require, promote and support coordination of stakeholder activities to achieve a coherent direction for information security. This will support the delivery of security education, training and awareness programs.

Principle 6: Review performance in relation to business outcomes

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

To review performance of information security from a governance perspective, the governing body should evaluate the performance of information security related to its business impact, not just effectiveness and efficiency of security controls. This can be done by performing mandated reviews of a performance measurement program for monitoring, audit, and improvement, and thereby link information security performance to business performance.

5.3 Processes

5.3.1 Overview

The governing body performs the "evaluate", "direct", "monitor" and "communicate" processes to govern information security. In addition, the "assure" process provides an independent and objective opinion about the governance of information security and the level attained. Figure 2 shows the relationship between these processes.

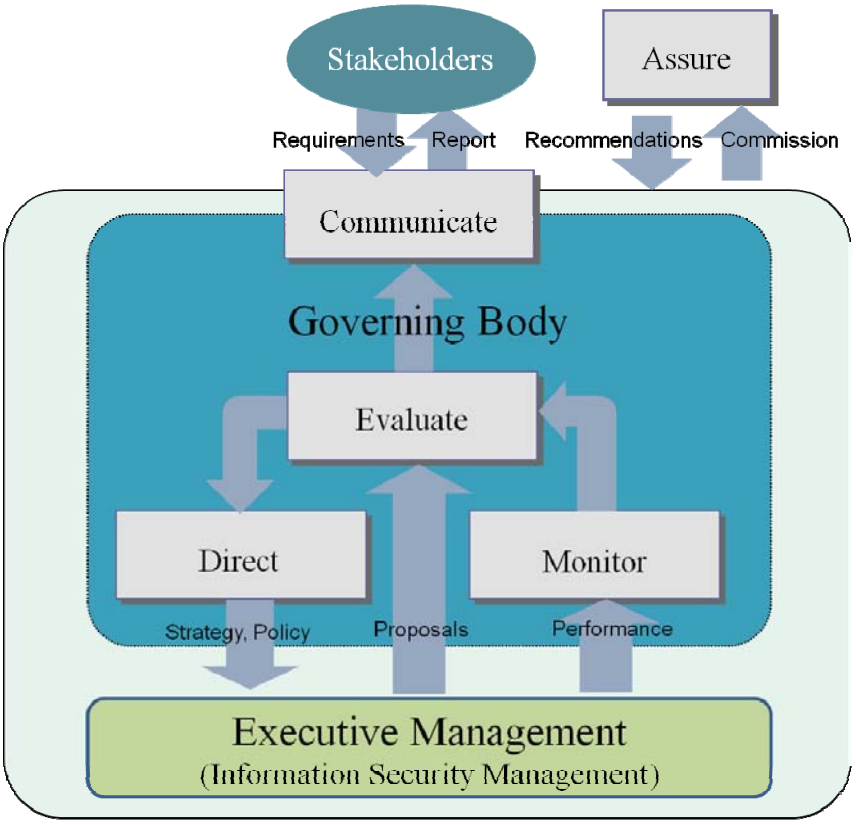

Figure 2 — Implementation of the governance model for information security

5.3.2 Evaluate

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

To perform the "evaluate" process, the governing body should:

- ensure that business initiatives take into account information security issues,
- respond to information security performance results, prioritize and initiate required actions.

To enable the “evaluate” process, executive management should:

- ensure that information security adequately supports and sustains the business objectives,
- submit new information security projects with significant impact to governing body.

5.3.3 Direct

“Direct” is the governance process, by which the governing body gives direction about the information security objectives and strategy that need to be implemented. Direction can include changes in resourcing levels, allocation of resources, prioritisation of activities, and approvals of policies, material risk acceptance and risk management plans.

To perform the “direct” process, the governing body should:

- determine the organisation’s risk appetite,
- approve the information security strategy and policy,
- allocate adequate investment and resources.

To enable the “direct” process, executive management should:

- develop and implement information security strategy and policy,
- align information security objectives with business objectives,
- promote a positive information security culture.

5.3.4 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:

- assess the effectiveness of information security management activities,
- ensure conformance with internal and external requirements,
- consider the changing business, legal and regulatory environment and their potential impact on information risk.

To enable the “monitor” process, executive management should:

- select appropriate performance metrics from a business perspective,
- provide feedback on information security performance results to the governing body including performance of action previously identified by governing body and their impacts on the organisation,
- alert the governing body of new developments affecting information risks and information security.

5.3.5 Communicate

“Communicate” is the bi-directional governance process by which the governing body and stakeholders exchange information about information security, appropriate to their specific needs.

One of the methods to “communicate” is information security status which explains information security activities and issues to stakeholders, examples of which are shown in Annexes A and B.

To perform the “communicate” process, the governing body should:

- report to external stakeholders that the organisation practices a level of information security commensurate with the nature of its business,
- notify executive management of the results of any external reviews that have identified information security issues, and request corrective actions,
- recognize regulatory obligations, stakeholders expectations, and business needs with regard to information security.

To enable the “communicate” process, executive management should:

- advise the governing body of any matters that require its attention and, possibly, decision,
- instruct relevant stakeholders on detailed actions to be taken in support of the governing body’s directives and decisions.

5.3.6 Assure

“Assure” is the governance process by which the governing body commissions independent and objective audits, reviews or certifications. These will identify and validate the objectives and actions related to carrying out governance activities and conducting operations in order to attain the desired level of information security.

To perform the “assure” process, the governing body should:

- commission independent and objective opinions of how it is complying with its accountability for the desired level of information security.

To enable the “assure” process, executive management should:

- support the audit, reviews or certifications commissioned by governing body.

Annex A
(informative)

An example of information security status

An organisation may develop an information security status and disclose it to stakeholders as a communication tool for information security.

The organisation should select and decide the format and the contents of the information security status. Annex A is an example that utilizes an information security audit statement for declaring satisfaction.

Table A.1 — An information security status

Management is satisfied that for the period **mmm** through **nnn** the information security controls and procedures, which are based on the criteria in **xyz** (e.g. ISO/IEC 27000 series, CobiT), relating to the organisation's operational procedures and systems supplemented by high level management controls were operating with sufficient effectiveness to provide reasonable assurance that defined information security control objectives in relation to confidentiality, integrity and availability were achieved. Management has provided **ABC**, as external information security auditors, with a representation letter to this effect. **ABC** were appointed by the board of directors to examine management's information security control assertion. Their examination was made in accordance with established standards, and included evaluating the design and operating effectiveness of information security controls and procedures through sample testing. In this regard, **ABC** issued an opinion to management that the results of their testing indicates that, with specific exceptions, based on the identified management criteria of **xyz** (e.g. ISO/IEC 27000 series, CobiT), controls were in material respects effective. Management's full assertion letter and the external audit report with any identified exceptions in relation to information security controls has been discussed with the audit committee and provided to all board members. Copies are available to shareholders upon request.

NOTE: "nnn", "mmm", "xyz", "ABC" are placeholders. Specific dates and names should appear in actual statements.

Annex B
(informative)

An example of detailed information security status

Annex B is an example of information security status disclosing detailed contents. It is particularly useful for organisations that expect to enhance their reputation by emphasizing their security, e.g. ICT businesses. Transparency of the organisation's approach to it's security risk and appropriate disclosure is also effective to increase trust. Common awareness can be shared among stakeholders through those activities.

Table B.1 — A detailed information security status

Introduction

- **Scope** (strategy, policies, standards), **perimeter** (geographic/organisational units), **period covered** (month/quarter/six months/year)

Overall status

- **Satisfactory/Not Yet Satisfactory/Unsatisfactory**

Updates (as appropriate and relevant)

- **Progress towards achieving the information security strategy**

  Elements completed/in-hand/planned

- **Changes in information security management system**

  ISMS policy revision, organisational structure to implement ISMS (including assignment of responsibilities)

- **Progress towards Certification**

  ISMS (re)certification, certified information security audits

- **Budgeting/staffing/training**

  Financial situation, headcount adequacy, information security qualifications

- **Other information security activities**

  Business continuity management involvement, awareness campaigns, internal/external audit assistance

Significant issues (if any)

- **Results of information security reviews**

  Recommendations, management responses, action plans, target dates

- **Progress in respect of major internal/external audit reports**

  Recommendations, management responses, action plans, target dates

- **Information security incidents**

  Estimated impact, action plans, target dates

- **(Non-)Compliance with related legislation and regulations**

  Estimated impact, action plans, target dates

Decision(s) required (if any)

- **Additional resources**

  To enable information security to support business initiative(s)

Bibliography

[1] ISO/IEC 27001:2005, *Information technology – Security techniques – Requirements of information security management systems*

[2] ISO/IEC 27002:2005, *Information technology – Security techniques – Code of practice for information security management*

[3] ISO/IEC 27005:2011, *Information technology – Security techniques – Information security risk management*

[4] ISO/IEC 38500:2008, *Corporate Governance of Information technology – A standard for corporate governance of information technology*

[5] ITU-T Recommendation X.1051 (2008) | ISO/IEC 27011:2008, *Information technology – Security techniques – Information security management guidelines for telecommunications organisations based on ISO/IEC 27002*

[6] ITGI, Information Security Governance framework: 2009

[7] ISF, Standard of Good Practice for Information Security: 2011

ICS 35.040

Price based on 11 pages