DRAFT INTERNATIONAL STANDARD ISO/IEC DIS 27014

ISO/IEC JTC **1** Secretariat: **ANSI**

Voting begins on
2011-11-11

Voting terminates on
2012-04-11

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION • МЕЖДУНАРОДНАЯ ОРГАНИЗАЦИЯ ПО СТАНДАРТИЗАЦИИ • ORGANISATION INTERNATIONALE DE NORMALISATION
INTERNATIONAL ELECTROTECHNICAL COMMISSION • МЕЖДУНАРОДНАЯ ЭЛЕКТРОТЕХНИЧЕСКАЯ КОММИСИЯ • COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

Information technology — Security techniques — Governance of information security

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

ICS 35.040

In accordance with the provisions of Council Resolution 21/1986 this DIS is circulated in the English language only.

Conformément aux dispositions de la Résolution du Conseil 21/1986, ce DIS est distribué en version anglaise seulement.

To expedite distribution, this document is circulated as received from the committee secretariat. ISO Central Secretariat work of editing and text composition will be undertaken at publication stage.

Pour accélérer la distribution, le présent document est distribué tel qu'il est parvenu du secrétariat du comité. Le travail de rédaction et de composition de texte sera effectué au Secrétariat central de l'ISO au stade de publication.

THIS DOCUMENT IS A DRAFT CIRCULATED FOR COMMENT AND APPROVAL. IT IS THEREFORE SUBJECT TO CHANGE AND MAY NOT BE REFERRED TO AS AN INTERNATIONAL STANDARD UNTIL PUBLISHED AS SUCH.

IN ADDITION TO THEIR EVALUATION AS BEING ACCEPTABLE FOR INDUSTRIAL, TECHNOLOGICAL, COMMERCIAL AND USER PURPOSES, DRAFT INTERNATIONAL STANDARDS MAY ON OCCASION HAVE TO BE CONSIDERED IN THE LIGHT OF THEIR POTENTIAL TO BECOME STANDARDS TO WHICH REFERENCE MAY BE MADE IN NATIONAL REGULATIONS.

RECIPIENTS OF THIS DRAFT ARE INVITED TO SUBMIT, WITH THEIR COMMENTS, NOTIFICATION OF ANY RELEVANT PATENT RIGHTS OF WHICH THEY ARE AWARE AND TO PROVIDE SUPPORTING DOCUMENTATION.

CONTENTS

Page

INTERNATIONAL STANDARD <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 Standardisation 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 standardising telecommunications on a world-wide basis. The World Telecommunication Standardisation 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, 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 concepts and guidance on principles and processes for the governance of information security, by which organisations can evaluate, direct and monitor the management of information security.

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 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 - Executive management is sometimes called top management and can include Chief Executive Officers, Chief Financial Officers, Chief Information Officers, and similar roles

3.2 **governing body:** person or group of people who are ultimately accountable for the performance of the organisation

> NOTE - Governing body can in some jurisdictions be a board of directors.

3.3 **governance of information security:** set of principles and processes by which an organisation provides direction and oversight of information security-related activities.

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 and acceptable, 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 strategy with business strategy /objectives (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 and regulatory)

4.4 Relationship

There are several other 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.

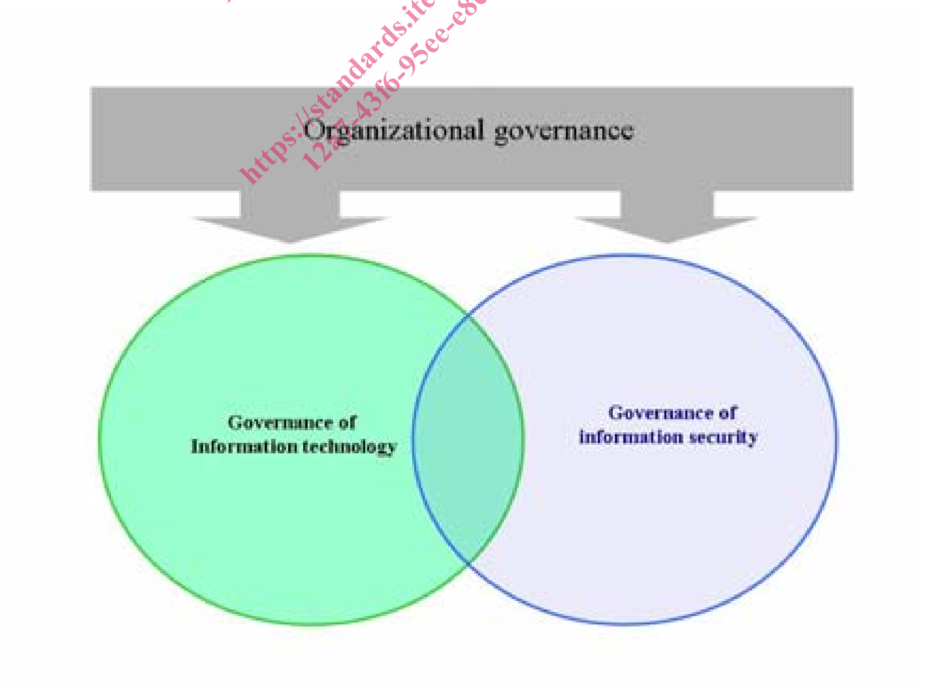
Organizational governance
Governance of Information technology
Governance of information security

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

Whereas the overarching scope of IT governance is aiming at resources required to acquire, process, store and disseminate information. However, the scope of information security governance is aiming at confidentiality, integrity and availability of information. Both governance schemes need to be handled by the following governance processes: EDM (Evaluate, Direct, Monitor).

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 activities 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 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 as appropriate IT perspectives. 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 both stored and 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 sufficient 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 a risk management appropriate to the organisation, it should be consistent and integrated with the organisation's overall risk management approach. The level of risk the organisation is prepared to accept needs to be approved and appropriate resources to implement risk management methods should be allocated by the governing body