International Telecommunication Union

ITU-T X.1054

(09/2012)

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

Information and network security – Security management

Information technology – Security techniques – Governance of information security

Recommendation ITU-T X.1054

ITU-T X-SERIES RECOMMENDATIONS

DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

PUBLIC DATA NETWORKS	X.1–X.199
OPEN SYSTEMS INTERCONNECTION	X.200–X.299
INTERWORKING BETWEEN NETWORKS	X.300–X.399
MESSAGE HANDLING SYSTEMS	X.400–X.499
DIRECTORY	X.500–X.599
OSI NETWORKING AND SYSTEM ASPECTS	X.600–X.699
OSI MANAGEMENT	X.700–X.799
SECURITY	X.800–X.849
OSI APPLICATIONS	X.850–X.899
OPEN DISTRIBUTED PROCESSING	X.900–X.999
INFORMATION AND NETWORK SECURITY	
General security aspects	X.1000–X.1029
Network security	X.1030–X.1049
Security management	**X.1050–X.1069**
Telebiometrics	X.1080–X.1099
SECURE APPLICATIONS AND SERVICES	
Multicast security	X.1100–X.1109
Home network security	X.1110–X.1119
Mobile security	X.1120–X.1139
Web security	X.1140–X.1149
Security protocols	X.1150–X.1159
Peer-to-peer security	X.1160–X.1169
Networked ID security	X.1170–X.1179
IPTV security	X.1180–X.1199
CYBERSPACE SECURITY	
Cybersecurity	X.1200–X.1229
Countering spam	X.1230–X.1249
Identity management	X.1250–X.1279
SECURE APPLICATIONS AND SERVICES	
Emergency communications	X.1300–X.1309
Ubiquitous sensor network security	X.1310–X.1339
CYBERSECURITY INFORMATION EXCHANGE	
Overview of cybersecurity	X.1500–X.1519
Vulnerability/state exchange	X.1520–X.1539
Event/incident/heuristics exchange	X.1540–X.1549
Exchange of policies	X.1550–X.1559
Heuristics and information request	X.1560–X.1569
Identification and discovery	X.1570–X.1579
Assured exchange	X.1580–X.1589

For further details, please refer to the list of ITU-T Recommendations.

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

Information technology – Security techniques – 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 has become a key issue for organizations. Not only are there increasing regulatory requirements, but also the failure of an organization's information security measures can have a direct impact on an organization's reputation.

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

In addition, governance of information security provides a powerful link between an organization'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 organization.

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 organization.

History

Edition	Recommendation	Approval	Study Group
1.0	ITU-T X.1054	2012-09-07	17

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, 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 TSB patent database at http://www.itu.int/ITU-T/ipr/.

CONTENTS

INTERNATIONAL STANDARD
RECOMMENDATION ITU-T

Information technology – Security techniques – Governance of information security

1 Scope

This Recommendation | International Standard provides concepts and guidance on principles and processes for the governance of information security, by which organizations can evaluate, direct and monitor the management of information security.

This Recommendation | International Standard is applicable to all types and sizes 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 27000:2009, *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 organization.

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

NOTE 2 – Executive management can include chief executive officers, 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 organization.

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 organization's information security-related activities are directed and controlled.

3.4 Stakeholder: Any person or organization that can affect, be affected by, or perceive themselves to be affected by an activity of the organization.

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 organization's decisions and the performance of the organization. In respect to information security, the key focus of the governing body is to ensure that the organization'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 organization, such as governance of information technology, and organizational governance. Every governance model is an integral component of the governance of an organization, 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.

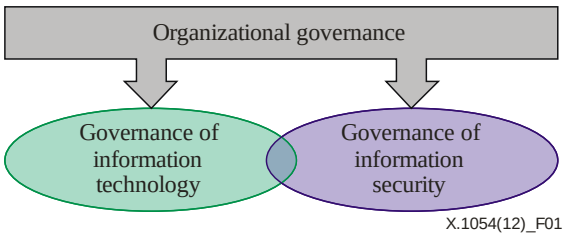

Figure 1 – Relationship between governance of information security and governance of information technology

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 governance 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 clauses.

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 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 organization 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 organization-wide information security

Governance of information security should ensure that information security activities are comprehensive and integrated. Information security should be handled at an organizational 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 organization-wide security, responsibility and accountability for information security should be established across the full span of an organization's activities. This regularly extends beyond the generally perceived 'borders' of the organization 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 organization, including loss of competitive advantage, compliance and liability risks, operational disruptions, reputational harm and financial loss.

To adopt information appropriate to the organization, it should be consistent and integrated with the organization's overall risk management approach. Acceptable levels of information security should be defined based upon the risk appetite of an organization, including the loss of competitive advantage, compliance and liability risks, operational disruptions, reputation 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 organizational objectives, the governing body should ensure that information security is integrated with existing organization 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 organization, 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.

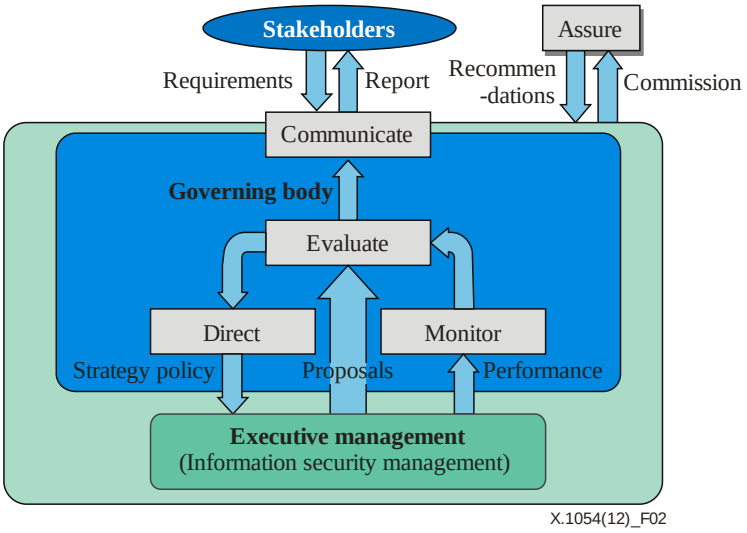

Figure 2 – Implementation of the governance model for information security

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 optimize 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, prioritization of activities, and approvals of policies, material risk acceptance and risk management plans.

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

- determine the organization'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 organization,
- alert the governing body of new developments affecting information risks and information security.

5.3.5 Communicate

"Communicate" is the bidirectional 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 organization 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 information concerning 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

An example of information security status

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

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

The organization 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 – 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., 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., 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

An example of detailed information security status

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

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

Table B – A detailed information security status

Introduction

- **Scope** (strategy, policies, standards), **perimeter** (geographic/organizational 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, organizational 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] Recommendation ITU-T X.1051 (2008) | ISO/IEC 27011:2008, *Information technology – Security techniques – Information security management guidelines for telecommunications organizations based on ISO/IEC 27002*.

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

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

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

[5] ISO/IEC 38500:2008, *Corporate Governance of Information technology*.

[6] ITGI, *Information Security Governance framework: 2009*.

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

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	General tariff principles
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Terminals and subjective and objective assessment methods
Series Q	Switching and signalling
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	**Data networks, open system communications and security**
Series Y	Global information infrastructure, Internet protocol aspects and next-generation networks
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2013