INTERNATIONAL STANDARD

ISO/IEC 30121

First edition
2015-03-15

Information technology — Governance of digital forensic risk framework

Technologies de l'information — Gouvernance du cadre de risque forensique numérique

Reference number
ISO/IEC 30121:2015(E)

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

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. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

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. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

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).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation on the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the WTO principles in the Technical Barriers to Trade (TBT), see the following URL: Foreword — Supplementary information.

The committee responsible for this document is ISO/IEC JTC 1, *Information technology*, Subcommittee SC 40, *IT Service Management and IT Governance*.

Introduction

Organizations of any kind face both internal and external factors and influences that can lead to the occurrence of legal actions and placement of demands on the Information Technology (IT) and related Information Systems (IS) to disclose digital evidence. The occurrence of legal action may be the result of an uncertain, unplanned, or unexpected event or it may occur as a planned course of action against employees, competitors, or service suppliers. Whether a risk is significant or not will depend on the level of risk and the organization's risk attitude. Its risk attitude will be reflected in its risk criteria. Because it is almost certain that digital evidence will be discovered and, therefore, be subject to legal disclosure, organizations should plan and develop capability to deal with such legal actions before they occur.

This International Standard is about the prudent strategic preparation for digital investigation of an organization. Forensic readiness assures that an organization has made the appropriate and relevant strategic preparation for accepting potential events of an evidential nature. Actions may occur as the result of inevitable security breaches, fraud, and reputation assertion. In every situation, IT should be strategically deployed to maximise the effectiveness of evidential availability, accessibility, and cost efficiency.

The responsibility of the Governing body is to provide strategic direction in all matters of relevance to the organization. The Governing body is informed by principles of best practice that provide general guidance on matters of certainty and compliance. These principles may come from legal mandates, standards, or social and cultural imperatives. In this International Standard, the principles come from ISO/IEC 38500 for the guidance of best practice for the governance of IT (Clause 4).

Principles require implementation. The tasks of governance are to evaluate proposals and plans, to monitor performance and conformance, and to direct strategy and policies. The stakeholders of an organization may provide the mandate for governance and the Governing body has the ultimate ownership of risk. A framework for the governance of digital forensic risk is established by the owners of risk taking appropriate actions to assure the strategic direction of the organization. Hence, the strategic objective is to implement the principles and to assure adequate preparation for digital investigation (Clause 5).

The framework requires strategic processes to deliver direction to executives and top managers. The strategic processes are selected to assure adequate scope and are principally archival, discovery, disclosure, capability, and risk criteria compliance (Clause 6).

The goals derived from the principles are measureable through Key Goal Indicators (KGIs), the strategic objectives derived from the strategies are measurable through the Key Performance Indicators (KPIs), and the variation between the KGIs and the KPIs measures is an indication of the organization's business performance (KBIs) (Clause 7).

This International Standard should be used in conjunction with the vocabulary contained in ISO Guide 73:2009; ISO/IEC 35802, *Information technology — Governance of IT framework and model*; and ISO/IEC 38500, *Information technology — Governance of IT for the organization*.

Information technology — Governance of digital forensic risk framework

1 Scope

This International Standard provides a framework for Governing bodies of organizations (including owners, board members, directors, partners, senior executives, or similar) on the best way to prepare an organization for digital investigations before they occur. This International Standard applies to the development of strategic processes (and decisions) relating to the retention, availability, access, and cost effectiveness of digital evidence disclosure. This International Standard is applicable to all types and sizes of organizations.

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 38500, *Information technology — Governance of IT for the organization*

ISO Guide 73:2009, *Risk management — Vocabulary*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 38500, ISO Guide 73:2009, and the following apply.

3.1
digital evidence
information or data stored or transmitted in binary form that may be relied upon as evidence

[SOURCE: ISO/IEC 27037:2012, 3.5]

3.2
Governing body
person or group of people who are accountable to stakeholders for the performance and conformance of the organization

[SOURCE: ISO/IEC TR 38502:2014, 2.9]

3.3
digital forensics
scientific tasks, techniques, and practices used in the investigation of stored or transmitted binary information or data for legal purposes

3.4
strategic risk
effect of uncertainty on goals

4 Principles

4.1 Responsibility

Individuals and groups within the organization understand and accept their responsibilities in respect of both supply of, and demand for digital evidence. Those with responsibility for investigations also have the skill, independence and authority to perform those actions.

4.2 Strategy

The organization's strategy development takes into account the current and future retention, availability, access to and cost effectiveness of digital evidence; the strategic plans for evidential capability satisfy the current and ongoing needs of the organization.

4.3 Acquisition

IT asset acquisitions are made to support the organization's strategies, on the basis of appropriate and ongoing analysis, with clear and transparent decision making. There is appropriate balance between benefits, opportunities, costs, and risks, in both the short term and the long term.

4.4 Performance

IT is fit for purpose in supporting the organization, providing the services, levels of service and service quality required to meet current and future organization digital evidence requirements.

4.5 Conformance

IT assets comply with all mandatory legislation and regulations. Policies and practices are clearly defined, implemented and enforced in accordance with the organization's risk criteria.

4.6 Human behaviour

Digital forensic policies, practices and decisions demonstrate respect for human behaviour, including the current and evolving needs of all the people in the organization's processes.

5 The framework

5.1 Stakeholder mandate

The Governing body should be constituted to represent the stakeholders, is to have the authority to set the strategic direction of the organization, and should establish the capabilities to function.

5.2 Establishment

The work cycle of the Governing body should be aligned with the tasks of Evaluate – Direct – Monitor; and to facilitate the adoption of strategic policy, strategic planning and strategic capability.

5.3 Evaluate

The Governing body should examine and make judgement on the current and future requirements for digital evidence, including strategies, proposals, plans and supply arrangements (whether internal, external, or both). In evaluating the use of IT, the requirement to produce digital evidence and the requirements for forensic processes should be assessed.

5.4 Direct

The Governing body should assign responsibility for, and direct preparation and implementation of strategies, plans and policies. Plans should set the strategic direction for digital evidence, IT operations and capabilities. Governing bodies should encourage a culture of good governance of IT in their organization by requiring managers to provide timely information, to comply with strategic directions and to conform to the risk criteria.

5.5 Monitor

The Governing body should monitor, through appropriate measurement systems, the performance and conformance of IT systems for digital evidence. They should reassure themselves that performance is in accordance with strategic plans and its levels of risk are within the organization's risk criteria. Responsibility for the effective, efficient and acceptable use of IT for evidential purposes by an organization, remains with the Governing body and cannot be delegated.

6 Processes

6.1 Archival strategy

An organization should establish a comprehensive archival retention of information properties. Archival processes should be structured, complete, efficient, secure, and maintain the integrity of the data.

6.2 Discovery strategy

An organization should establish efficient and effective information retrieval capabilities. Accurate and timely access to organization information is critical for decision-making and the presentation of evidence.

6.3 Disclosure strategy

An organization should establish criteria for the securing and the disclosing of information. For any assessment of the digital-related risk that the organization faces, it should apply its risk criteria to determine if the level of risk is acceptable or whether the adoption of further strategic risk is required. Information that is disclosed should be preserved so that it is auditable.

6.4 Digital forensic capability strategy

An organization should adopt policies and plans to assure the preservation of digital evidence and the retention of and/or access to digital forensic skills. The organization should maintain processes that assure the integrity of investigations, the independence of experts, and the evidential value of binary information.

6.5 Risk compliance strategy

An organization should make decisions on whether to adopt strategic risk based on the application of its risk criteria for digital evidence. The Governing body should gain assurance that the level of risk remains within the organizations risk criteria.

7 Metrics

7.1 General

An organization should measure the critical attributes of the entity in order to evaluate proposals and plans, to monitor performance and conformance, and to direct strategy and policies. Reports provide the organization's Governing body with the information on which to make informed decisions.

7.2 Key goal indicators

A Key Goal Indicator (KGI) reports the measurement of attributes from goals. The KGI provides a way to monitor the achievement of the principle values.

7.3 Key performance indicators

A Key Performance Indicator (KPI) reports the measurement of attributes from objectives. The KPI provides a way to monitor the achievement of the process values.

7.4 Key business indicators

A Key Business Indicator (KBI) reports the variation between a Key Goal Indicator and a Key Performance Indicator. The KBI provides a way to monitor the achievement of organization progress.

Annex A
(informative)

International Standard overview

The International Standard overview is shown in Figure A.1.

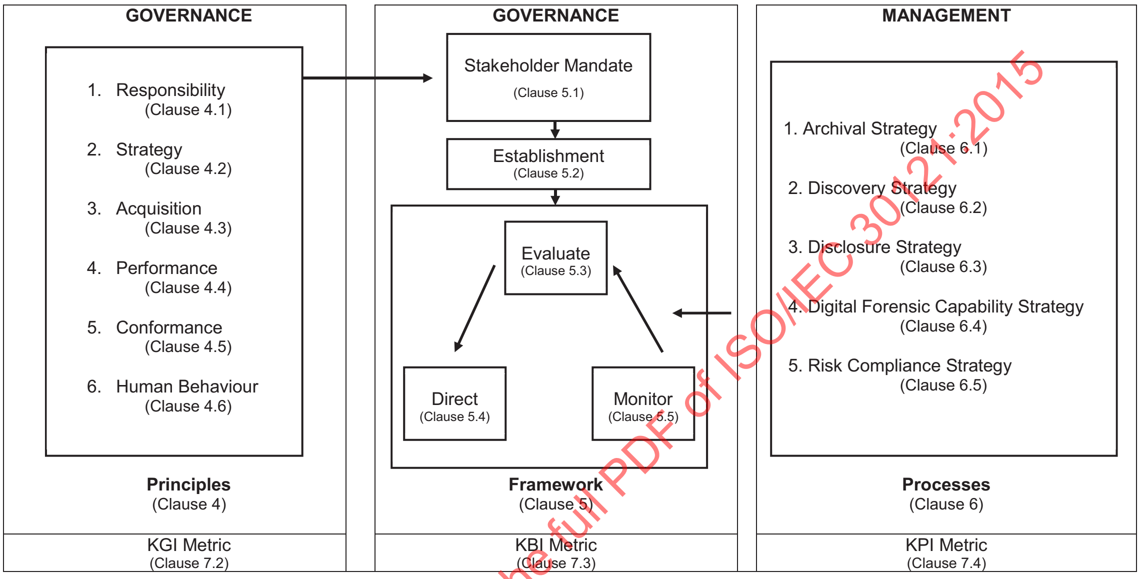
GOVERNANCE
1. Responsibility (Clause 4.1)
2. Strategy (Clause 4.2)
3. Acquisition (Clause 4.3)
4. Performance (Clause 4.4)
5. Conformance (Clause 4.5)
6. Human Behaviour (Clause 4.6)
Principles (Clause 4)
KGI Metric (Clause 7.2)
GOVERNANCE
Stakeholder Mandate (Clause 5.1)
Establishment (Clause 5.2)
Evaluate (Clause 5.3)
Direct (Clause 5.4)
Monitor (Clause 5.5)
Framework (Clause 5)
KBI Metric (Clause 7.3)
MANAGEMENT
1. Archival Strategy (Clause 6.1)
2. Discovery Strategy (Clause 6.2)
3. Disclosure Strategy (Clause 6.3)
4. Digital Forensic Capability Strategy (Clause 6.4)
5. Risk Compliance Strategy (Clause 6.5)
Processes (Clause 6)
KPI Metric (Clause 7.4)

Figure A.1 — International Standard Overview