INTERNATIONAL STANDARD

ISO
24143

Information and documentation — Information Governance — Concept and principles

Information et documentation — Gouvernance de l'information — Concept et principes

iTeh STANDARD PREVIEW
(standards.iteh.ai)

ISO 24143:2022
https://standards.iteh.ai/catalog/standards/sist/9facb9f0-4106-4eeb-8ba8-f17558cd4cd9/iso-24143-2022

Contents

Page

iii

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

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 ISO documents 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 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 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.

This document was prepared by Technical Committee ISO/TC 46, *Information and documentation*.

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.

Introduction

Information is a critical asset that is indispensable to support business processes and therefore, a foundation for the success of any business activities. Due to numerous existing and emerging forms and uses of information and information-related risks, organizations often struggle with implementing consistent and comprehensive systems to store, retrieve, share and analyse information. The current global digital transformation and the changes in societal expectations increasingly demand greater transparency, accountability, data protection, security, interoperability and information sharing within and between organisations. This trend requires a solid vision and strategy for Information Governance that supports the business process at a strategic level including digital transformation initiatives. Many governmental and non-governmental organisations worldwide already perceive the necessity and understand the benefits of coordinating at a strategic level the efforts of multiple information-, data- and knowledge-related disciplines.

This document defines concepts and principles for Information Governance.

This document provides guiding principles for members of governing bodies of organisations (which can comprise owners, directors, partners, executive managers, or similar) on the effective, efficient, compliant, secure, transparent and accountable creation, use, maintenance, preservation and disposition of information within their organisations.

Information Governance is an integral part of the overall governance of the organisation. It identifies common high-level principles and provides a framework enabling effective and efficient cooperation of all the information-related professionals, in support of the mission of an organisation and achievement of its strategic goals. Stakeholders which are engaged in the collaboration include but are not limited to:

— Data Management

— Information Management

— Records Management

— Knowledge Management

— Regulatory Compliance

— Digital Preservation

— Information Security

— Enterprise Architecture

— Data Protection

— Open Data

— Big Data

— Artificial Intelligence (AI)

— Blockchain

— Business Processes

— Quality Management.

Information Governance requires coherence and integration with relevant Management System Standards (MSS), such as ISO 9000, ISO/IEC 27000 and the ISO 30300 series.

Information Governance is a strategic framework for managing information assets across an entire organisation to support its business outcomes and obtain assurance that the risks to its information, and thereby the operational capabilities and integrity of the organisation, are adequately identified

and managed. Information Governance includes but is not limited to policies, processes, procedures, roles and controls put in place to meet regulatory, legal, risk and operational requirements. Information Governance provides an overarching high-level framework that:

— aligns all information-related activities with the mission and goals of an organisation, and its business, legal and societal obligations,

— ensures a comprehensive and systematic approach to information by integrating processes relevant to directing and controlling information,

— supports cooperation between stakeholders, and

— creates a high-level basis for managing information regardless its form, type and format, informs education, professional development of the workforce and awareness about information-related obligations, risks and possibilities.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

ISO 24143:2022
https://standards.iteh.ai/catalog/standards/sist/9facb9f0-4106-4eeb-8ba8-f17558cd4cd9/iso-24143-2022

Information and documentation — Information Governance — Concept and principles

1   Scope

This document establishes concepts and principles for Information Governance.

This document applies to the governance of the organisation's past, current and future information assets. It applies to organisations of all sizes in all sectors, including public and private companies, government entities, and not-for-profit organisations.

2   Normative references

There are no normative references in this document.

3   Terms and definitions

For the purposes of this document, the following terms and definitions apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at https://www.electropedia.org/

3.1   Terms relating to concept of information

3.1.1
authentic (preferred term)
authenticity (admitted term)
property of *information* (3.1.3) that can be proven to be what it purports to be

Note 1 to entry: Authenticity implies that information has been created or sent by the agent purported to have created or sent it, and to have been created or sent when purported.

Note 2 to entry: When information can be proven to be what it purports to be it, it can be called authentic information.

Note 3 to entry: See Figure A.1 in Annex A.

[SOURCE: ISO 30300:2020, 3.2.2, modified — "records" has been replaced by "information". "Authentic" has been replaced by "authenticity". A new Note 2 to entry has been added.]

3.1.2
data
set of characters or symbols to which meaning is or could be assigned

Note 1 to entry: See Figure A.1 in Annex A.

[SOURCE: ISO 30300: 2020, 3.2.4]

1

3.1.3
information
data ([3.1.2](#)) in context with a particular meaning

Note 1 to entry: See [Figure A.1](#) in [Annex A](#).

[SOURCE: ISO 30300:2020, 3.2.7]

3.1.4
information asset
information ([3.1.3](#)) that has value to the relevant stakeholder

Note 1 to entry: See [Figure A.1](#) in [Annex A](#).

[SOURCE: ISO/TS 17573-2:2020, 3.95, modified — "information" is taken place of "knowledge and data".]

3.1.5
integrity
property of information that is complete and unaltered

Note 1 to entry: See [Figure A.1](#) in [Annex A](#).

[SOURCE: ISO 30300:2020, 3.2.8, modified — "records" has been replaced by "information".]

3.2 Terms relating to the concept of Information Governance

3.2.1
compliance
characteristic of conformance to rules, such as those defined by a law, a regulation, a standard, or a policy

Note 1 to entry: See [Figure A.2](#) in [Annex A](#).

[SOURCE: ISO/IEC 20924:2021, 3.1.10, modified — The word "characteristic" has been added in the definition. A note to entry has been added.]

3.2.2
digital continuity
ability to use digital *information* ([3.1.3](#)) in the way that is needed, for whenever and wherever is needed

Note 1 to entry: See [Figure A.2](#) in [Annex A](#).

3.2.3
disposition
range of processes associated with implementing retention, destruction or transfer decisions about *information* ([3.1.3](#))

Note 1 to entry: See [Figure A.2](#) in [Annex A](#).

[SOURCE: ISO 30300:2020, 3.4.8, modified — "records" has been replaced by "information", shortened in words but keeping the meaning.]

3.2.4
e-discovery
process of identifying, collecting, preserving, reviewing and exchanging electronically stored information (ESI) for the purpose of using it as digital evidence

Note 1 to entry: E-discovery also known as ediscovery, eDiscovery, e-Discovery, e-discovery, electronic discovery.

Note 2 to entry: ESI includes, but not limited to electronic formats, emails, documents, presentations, databases, voicemail, audio and video files.

Note 3 to entry: E-discovery often refers to a form of digital investigation that attempts to find evidence in ESI in response to a request for production in a law suit or investigation.

Note 4 to entry: See Figure A.2 in Annex A.

3.2.5
framework
structure composed of related parts designed to support the accomplishment of a specific task

Note 1 to entry: See Figure A.2 in Annex A.

[SOURCE: ISO 15638-6:2014, 4.30]

3.2.6
governance
principles, policies and framework by which an organisation is directed and controlled

Note 1 to entry: See Figure A.2 in Annex A.

[SOURCE: ISO/IEEE 11073-10201:2020, 3.1.25, modified — "composed of related parts" taking place of "processes and specifications"]

3.2.7
Information Governance
strategic framework for governing *information assets* (3.1.4) across an entire organization in order to enhance coordinated support for the achievement of business outcomes and obtain assurance that the risks to its *information* (3.1.3), and thereby the operation capabilities and *integrity* (3.1.5) of the organisation, are effectively identified and managed

Note 1 to entry: Information Governance includes (but is not limited to) policies, processes, procedures, roles and controls put in place to meet regulatory, legal, risk and operational requirements.

Note 2 to entry: Data is one form of information asset.

Note 3 to entry: See Figure A.2 in Annex A.

3.2.8
information security
preservation of confidentiality, integrity and availability of *information* (3.1.3)

Note 1 to entry: See Figure A.2 in Annex A.

[SOURCE: ISO/IEC 27000:2018, 2.28]

4 Benefits of Information Governance

4.1 General

Information Governance is a strategic, multi-disciplinary framework enabling collaboration between related professions. It considers information as a valuable corporate asset, and has the potential to deliver the following benefits.

4.2 Strategic benefits

Information Governance:

a) Provides an overarching high-level governance framework that supports an organisation's mission and results in achieving economic and strategic benefits including, but not limited to:

  1) maximisation of value derived from the information assets,

    2) protection of the rights of the organisation and other stakeholders,

    3) compliance with legal and regulatory requirements, and

    4) promotion of openness, transparency and accountability;

b) Supports informed decision-making by providing timely access to authentic, reliable, relevant, full and accurate, current and accessible information;

c) Reduces risk that could cause reputational damage, financial loss or penalties by

    1) applying adequate security and protection to valuable information assets, and

    2) destroying or purging information that is no longer required to be retained;

d) Identifies gaps in systems, policies, procedures and processes required to govern an organisation's information assets effectively;

e) Ensures the organisation's policies are consistent and working in harmony with regards to security, privacy, appraisal, preservation, disposition, discovery and disclosure of information;

f) Provides a mechanism for inclusion of all information assets in the governance program;

g) Eliminates silos and professional frictions and encourages a cooperative and cross-disciplinary approach in implementing innovative and emerging technologies that align to organisational strategic objectives and priorities;

h) Supports ethical governance relating to existing and emerging technologies such as AI and block chain.

4.3 Operational benefits

Information Governance:

a) Provides a comprehensive and systematic approach to governing information that underpins an organisation's operation by integrating information management, information security and privacy, compliance, business continuity, disaster recovery, e-discovery and other aspects relevant to directing and controlling information;

b) Identifies what organisational information exists, where it is located, what actions can be taken on it, and how it should be managed and controlled, resulting in valuable information which can be used and reused many times;

c) Underpins systematic organisation of information assets, which allows increased availability, sharing and collaboration, and provides faster search and retrieval of business information;

d) Provides the framework for information assets maintenance to eliminate the loss of crucial business information;

e) Reduces costs associated with storing and the resources required to manage or discover information by adopting a disposition program that destroys information no longer needed or required to be retained;

f) Reduces the production cost for e-discovery and ensures that organisations are not creating additional risk by producing and retaining more information than necessary;

g) Preserves corporate culture and memory by providing a foundation for enhancing the capability of digital continuity collaboratively achieved at an enterprise level.

5 Principles of Information Governance

5.1 Recognising information as a corporate, strategic asset

Information Governance considers the organisation's information as an asset (as defined in 3.2.8). Information is strategic for the future of any organisation and facilitates its long-term sustainability.

Information Governance acknowledges legal, business, historical and other value of information and information assets, their essential role in business and governance, information-related benefits and risks, and the potential of information assets to become a key competitive advantage.

Information to be governed includes structured and unstructured, non-digital and digital information, as well as the information in the heads of the people.

5.2 Designing Information Governance as a key element of corporate strategy

Information Governance includes all the high-level, strategic aspects of governing and controlling information, such as the provision of infrastructure and systems for processing; compliance to legal and regulatory requirements related to information; governance instruments such as policies, procedures, and standards; and people (resourcing, training and professional development).

5.3 Integrating Information Governance into the organisation's governance frameworks

Information Governance should be included into the corporate governance: system by which corporations are directed and controlled (see ISO/IEC 38500), to achieve the organisation's goals, and to answer ethical requirements of integrity, memory and societal responsibility.

Information Governance forms an integral part of, and should be integrated with, all the organisation's governance frameworks and management systems. Information Governance integrates with all information management frameworks and systems, such as financial, risk, security, quality, environmental, health and safety management processes and their operational requirements and procedures. Information Governance should be included in the integrated reporting of the organisation.

Information Governance should encompass all information-centric governance facets or domains including but not limited to records management, data protection/privacy, information security, information sensitivity, data management, enterprise content management, document control and e-discovery.

5.4 Securing senior management's leadership and commitment

Senior management should be committed to guide, lead and support Information Governance. A member of the organisation's senior management should be responsible for Information Governance and ensure accountability, reporting to the most senior person or governance structure in the organisation.

The responsibilities of that Information Governance leader should include identifying the components of the organisation's Information Governance framework, defining the processes, procedures and driving them, unlocking potential and emergent obstacles, communicating the goals and business objectives, allocating the resources needed (team, structures, infrastructures) and keeping upper management informed on progress.

The Information Governance leader oversees all these activities together in a coherent Information Governance program.

In addition, the operational responsibility of Information Governance aspects can be delegated to an Information Governance officer, and/or other staff members at an appropriate level.