Examples of ISO/IEC Standards by Topic Area

May 11, 2022

Cybersecurity

1. ISO/IEC 27001
   This standard describes how to manage information security programs for an organization of any size, scope, and complexity. Organizations can undergo a certification process for conformance to ISO/IEC 27001. This standard is used in conjunction with information security controls and is most frequently used together with ISO/IEC 27002.

2. ISO/IEC 27002
   This standard is a comprehensive catalog of information security controls that provides high-level guidance for each control. It is frequently used with ISO/IEC 27001 but is also used by organizations as a primary set of information security guidelines.

3. ISO/IEC 27017
   Built on top of ISO/IEC 27002, this standard provides specific cloud security controls and is used either with ISO/IEC 27001, as an extension to ISO/IEC 27002, or as standalone guidance specifically for cloud controls.

4. ISO 31000, ISO/IEC 31010, and the second version of ISO/IEC 27005 (under development)
   ISO 31000 describes how to manage risk management programs for an organization of any size, scope, and complexity; ISO/IEC 31010 provides guidance on risk assessment techniques. ISO/IEC 27005 (which is under revision) provides guidance on how to manage information security risks based on ISO/IEC 27001 and ISO 31000.

5. ISO/IEC 29147 and ISO/IEC 30111
   This standard provides guidance for systems and software development organizations regarding how to inform customers about newly discovered vulnerabilities in the solutions that they acquired and integrated into their digital infrastructures.

6. ISO/IEC 15408
   This standard provides the basis for certifying that security functions within digital products are designed and are functioning as expected. These requirements are used for Common Criteria Certification, which is frequently requested for government procurement in many jurisdictions. Common Criteria certification is supported by a number of other additional standards. (https://commoncriteriaportal.org/)

7. ISO/IEC 27036 – Parts 1 through 4
   This is a multi-part standard that provides guidance for managing risks from supplier relationships to organization's business, data, and systems. These documents cover general requirements, guidelines for information and communication technology products and services, and guidelines for cloud services.

8. Note that there are a variety of ISO/IEC cryptography standards (e.g., symmetric key, public key-based). Examples include ISO/IEC 18033-X, 9797-X. ("-X" indicates a multi-part standard.)

Privacy

1. ISO/IEC 27018
   This standard provides cloud-specific privacy controls. These controls are an extension to the information security controls in ISO/IEC 27002.

2. ISO/IEC 29100
   This standard provides a privacy framework and defines key terms, such as personally identifiable information (PII) controller and PII processor.

3. ISO/IEC 27701
   This standard is an extension to ISO/IEC 27001 and ISO/IEC 27002 and provides controls for managing personal information within the context of an organization. Organizations may be a "PII controller" and/or a "PII processor" (as defined by ISO/IEC 29100).

4. ISO/IEC 20889
   This standard defines terms for de-identifying personal data as well as descriptions of techniques.

5. ISO/IEC 27555
   This standard provides guidelines for deleting personal data and includes descriptions of different methods.

6. Note that the risk management and cryptography standards listed under "Cybersecurity" above (4 & 8) are also relevant standards for privacy.

Internet of Things (IoT)

1. ISO/IEC 20924
   This standard provides the terms and definitions used in various IoT standards.

2. ISO/IEC 30141
   This standard is a reference document that defines an IoT systems architecture that should be used when developing an IoT system.

3. Under development: ISO/IEC 27402
   This standard provides a baseline set of security and privacy requirements for all IoT devices.

4. ISO/IEC 27400
   This standard provides security and privacy guidance for the various roles/stakeholders in IoT systems.

Artificial Intelligence (AI)

1. ISO/IEC 24028
   This technical report provides information related to trustworthiness in AI systems including transparency, explainability, controllability, threats, risks, resiliency, reliability, safety, security and privacy.

2. ISO/IEC 22989

   This standard provides the foundational terms and definitions for artificial intelligence along with descriptions of important concepts (e.g., lifecycle, trustworthiness, bias, neural networks, data).

3. ISO/IEC 24027

   This technical report provides information about bias in relation to AI systems including techniques and methods for assessing bias.

4. Under development: ISO/IEC 24368

   This technical report provides a high-level overview of the area of ethics and societal concerns relative to artificial intelligence including principles, processes and methods in this area.

5. Under development: ISO/IEC 4213

   This technical specification specifies methodologies for measuring classification performance of machine learning models, systems and algorithms.

6. Under development: ISO/IEC 5259

   This multipart standard covers methods and measures for the quality of data for analytics and machine learning. It covers determining, managing, labeling and reporting data quality.

7. Under development: ISO/IEC 5339

   This standard provides a set of guidelines for identifying the context, opportunities, and processes for developing and applying AI applications.

8. Under development: ISO/IEC 5469

   This technical report describes the properties, related risk factors, available methods and processes relating to AI functional safety.

9. Under development: ISO/IEC 6254

   This technical specification describes the objectives and methods for explainability of machine learning (ML) models and AI systems.

10. ISO/IEC 23053

    This standard provides an overview of machine learning including neural networks.

11. Under development: ISO/IEC 23894

    This standard provides guidance to organizations on incorporating the development and use of AI into their overall risk management system.

12. ISO/IEC 38507

    This standard provides guidance to organizations on what information about the development and use of AI systems should be provided to its governing body (e.g., C-suite executives, Board of Directors) and the related responsibilities of the governing body.

13. Under development: ISO/IEC 42001

This standard provides requirements for establishing a management system for the development and use of AI systems in an organization along with guidance on controls that can be used to measure the effectiveness of related management processes.

Biometrics

1. ISO/IEC 2382-37

   This standard provides a systematic description of biometric terms and concepts.

2. ISO/IEC 19795-1

   This standard establishes requirements for testing the accuracy and throughput of biometric systems.

3. ISO/IEC 22116

   This technical report is a study of how age, ethnicity, and gender/sex impact the performance of face, fingerprint, and iris recognition systems.

4. Under development: ISO/IEC 19795-10

   This standard establishes requirements for evaluating fairness for biometric systems by quantifying biometric system performance variation across demographic groups.

5. Under development: ISO/IEC 9868

   This standard establishes recommendations and requirements for remote biometric identification systems, including both real-time and ex-post and AI-based systems.