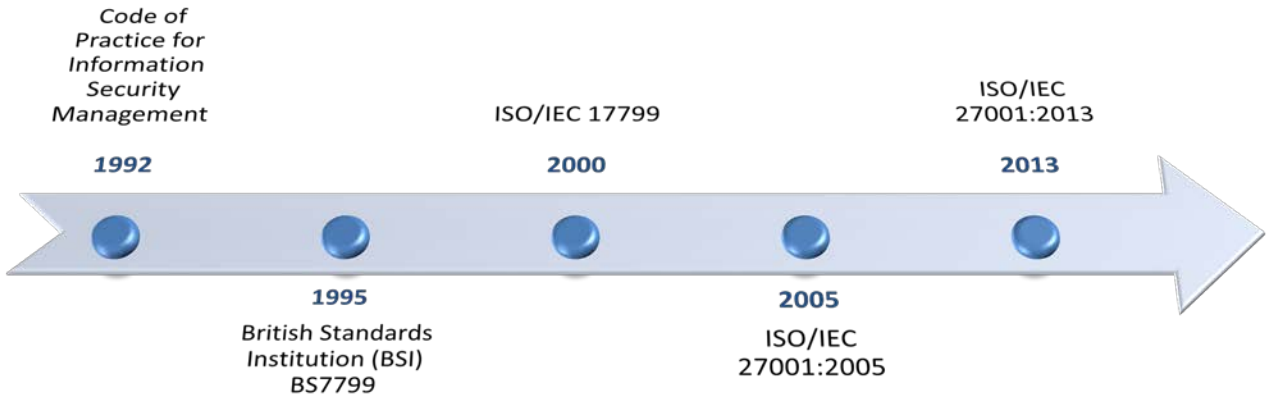
An Overview of ISO/IEC 27000 family of Information Security Management System Standards



What is ISO/IEC 27001?

The ISO/IEC 27001 standard, published by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), is known as "Information technology — Security techniques — Information security management systems — Requirements". ISO/IEC 27001:2013 (hereafter referred to as ISO/IEC 27001) is the most recent edition of ISO/IEC 27001 standard which revises the previous edition published in 2005 (ISO/IEC 27001:2005). ISO/IEC 27001 specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system (ISMS). The ISMS presents a systematic approach to keep sensitive information secure. It manages people, processes and IT systems through applying risk management processes. The ISMS suits not only large organisations but also small and medium businesses.

ISO/IEC 27001 is designed to be used in conjunction with supporting controls, an example of which is published in document, ISO/IEC 27002:2013 (hereafter referred to as ISO/IEC 27002). ISO/IEC 27002 details 114 security controls which are organised into 14 sections and 35 control objectives. The table of contents from ISO/IEC 27001 and ISO/IEC 27002 are provided in Appendix A.

Compliance with ISO/IEC 27001 can be formally assessed and certified by an accredited certification body. An organisation's ISMS certified against the ISO/IEC 27001 standard demonstrates an organisation's commitment to information security and provides confidence to their customers, partners and stakeholders.

ISO/IEC 27001 Certification Requirements

To meet ISO/IEC 27001 certification requirements, an organisation's ISMS must be audited by an internationally accredited certification body. Requirements in sections 4 to 10 in the ISO/IEC 27001 (see Appendix A) are mandatory requirements with no exclusion allowed. Having passed the formal audit, the certification body awards an organisation with an ISO/IEC 27001 certificate for its ISMS. The ISO/IEC 27001 certificate is valid for 3 years, after which the ISMS needs to be re-certified.

During the 3-year validity period, an organisation must perform certificate maintenance so as to confirm the ISMS remains compliant, operates as specified, and continually improves. To maintain the certification, the certification body will visit the ISMS site at least once a year to carry out a surveillance audit. During the surveillance audit, only a portion of the ISMS will be audited. Towards the end of the 3-year period, the certification body audits the entire ISMS.

An Overview of ISO/IEC 27000 family of Information Security Management System Standards

Benefits of ISO/IEC 27001 Certification

An organisation certified with ISO/IEC 27001 will bring benefits to its internal security as well as its external competitiveness.

Internally, by adopting the ISO/IEC 27001, an organisation can:

- Form a basis to enable the secure exchange of information and to protect data privacy, in particular relating to sensitive information;
- Manage and lower risk exposure, hence less chance of incidents being realised and in turn reducing time and money spent on responding to incidents;
- Strengthen the internal organisation and improve the security structure of the business, such as to clearly define responsibilities and duties related to information security;
- Reduce the resources needed for completing security-related information in bidding for contracts, as well as on-going submission after the contracts awarded, as required by clients.

Externally, by publicising the fact that ISO/IEC 27001 is certified, an organisation can:

- Provide customers and stakeholders with confidence in how it manages risks and security of their sensitive information;
- Facilitate compliance with legal obligations such as the Personal Data (Privacy) Ordinance (PD(P)O);
- Receive a competitive advantage, which assists the organisation to attract more investors and customers as a result;
- Improve consistency in the delivery of its services and products, thus enhancing customer satisfaction and client retention;
- Safeguard and enhance the organisation's reputation as its security processes have been validated by an independent certification body, and hence improve protection to the organisation, assets, shareholders and directors;
- Better prepare to face ever-increasing customer expectations. Nowadays the community is becoming more sensitive to information security incidents. Certification to a recognised international standard may gradually become a pre-requisite imposed by many customers.

Certification Bodies

The ISO/IEC 27001 certification process involves the accreditation of certification bodies. Such accreditation is granted to organisations who have demonstrated that they fully meet the requirements of the international standards ISO/IEC 17021 "Conformity assessment – Requirements for bodies providing audit and certification of management systems" and ISO/IEC 27006 "Requirements for bodies providing audit and certification of information security management systems".

Accreditation service for ISO/IEC 27001 certification was officially launched by Hong Kong Accreditation Service (HKAS) on 15 November 2011. Certification bodies can contact HKAS and apply for accreditation on a voluntary basis.

Costs for Certification

For initial certification, it includes the costs for both implementing the ISMS and certifying the ISO/IEC 27001. The cost of implementation depends largely on the gaps between the existing security controls and the required controls within the organisation. In terms of costs to implement, there are costs and resources for implementing security controls, writing documentation, training staff, etc. For the certification itself, it includes the cost of the external auditors (that charge a certain rate per day), application fees, certificate fees and maintenance fees, etc.

Adoption in Hong Kong

According to ISO Survey 2019, at least 36 362 ISO/IEC 27001 certificates have been issued in 133 countries and economies worldwide. In 2019, the top three countries for the total number of certificates issued were China (8 356), Japan (5 245) and the United Kingdom of Great Britain and Northern Ireland (2 818). From the information of the same survey, the number of certificates acquired in Hong Kong was 158. The number included some government departments certified against ISO/IEC 27001 for specific functional areas.

An Overview of ISO/IEC 27000 family of Information Security Management System Standards

Overview of the ISO/IEC 27001 Implementation and Certification process

- **ISO/IEC 27001 Implementation**

1. **Define information security policy**
   - Task: Identify business objectives and obtain management support to implement a security improvement program
2. **Define scope of the ISMS**
   - Task: Compare the existing information security management system against the requirements of ISO/IEC 27001 and select what business units, departments or systems are to be covered by the ISMS
3. **Perform a risk assessment**
   - Task: Define a method of risk assessment, inventory the information assets to protect, and rank assets according to risk classification based on risk assessment
4. **Manage the identified risk**
   - Task: Create a risk treatment plan to identify appropriate management actions, resources, responsibilities and priorities for managing information security risks
5. **Select controls to be implemented**
   - Task: Prepare a Statement of Applicability (SoA) to document which of the controls (e.g. the 114 security controls from ISO/IEC 27002) that are applicable to the ISMS and the way they will be implemented
6. **Implement controls**
   - Task: Develop programs to implement the identified controls

- **ISO/IEC 27001 Certification**

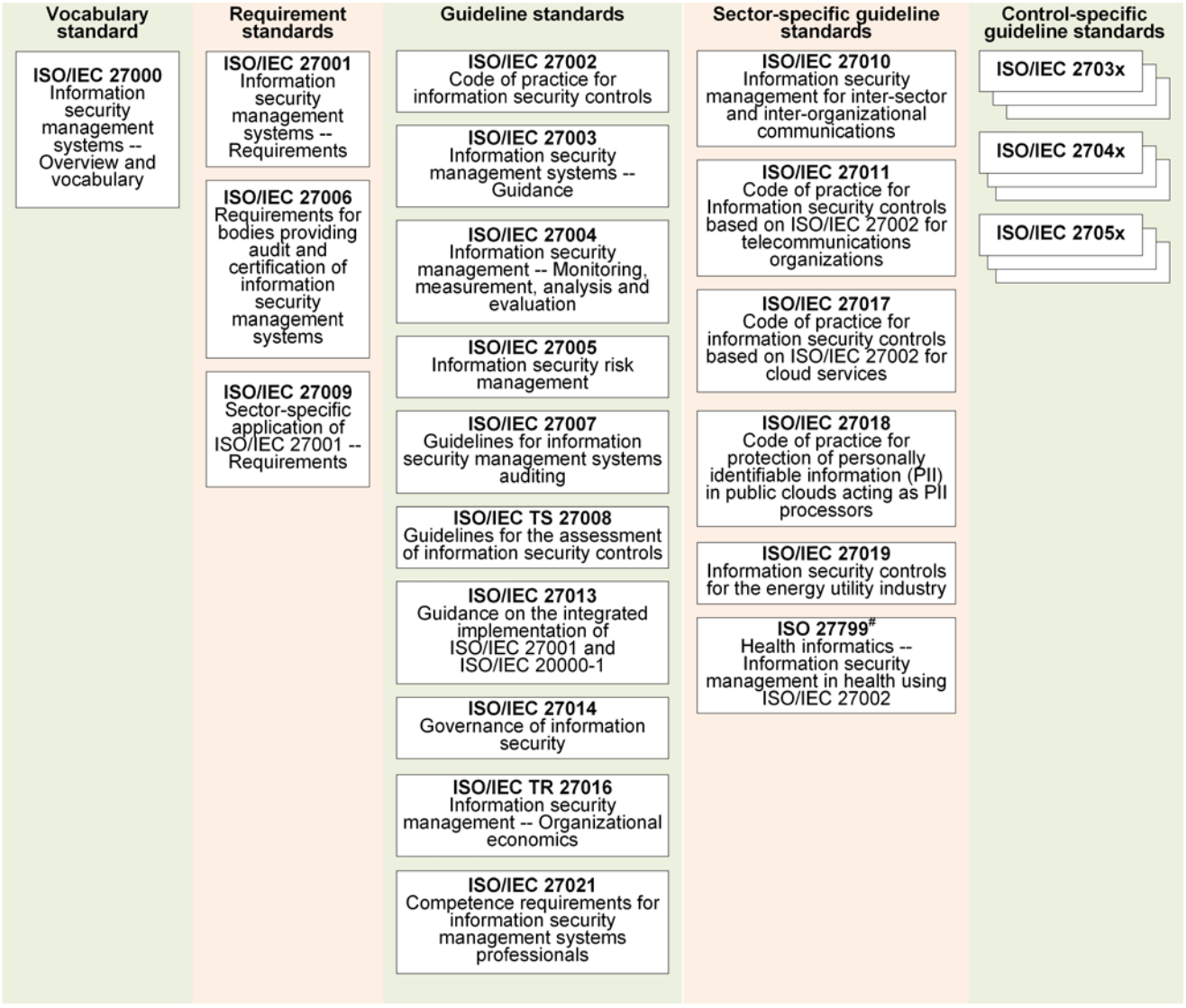
7. **Prepare for certification**
   - Task: Operate the ISMS and conduct a full cycle of internal audits, management reviews and activities
8. **Apply for certification**
   - Task: Proceed to certification application which includes stages of document review and on-site compliance audit

An Overview of ISO/IEC 27000 family of Information Security Management System Standards

Family of ISO/IEC 27000

The ISO/IEC 27000 family of standards (see Appendix B) consists of inter-related standards and guidelines, already published or under development, and contains a number of significant structural components. These components are focused upon normative standards describing ISMS requirements (ISO/IEC 27001), certification body requirements (ISO/IEC 27006) for those certifying conformity with ISO/IEC 27001, and additional requirement framework for sector-specific implementations of the ISMS (ISO/IEC 27009). Other standards and guidelines provide guidance for various aspects of an ISMS implementation, addressing a generic process as well as sector-specific guidance.

ISO/IEC 27000 Family of Standards Relationships



Notes:
International Standards not under the same general title that are also part of the ISO/IEC 27000 family of standards.

An Overview of ISO/IEC 27000 family of Information Security Management System Standards

The current version of ISO/IEC 27001 was released in 2013. Apart from the most mentioned ISO/IEC 27001, ISO/IEC 27002 and ISO/IEC 27018, some other standards in the ISO/IEC 27000 family are also being widely referenced. Some examples are:

- ISO/IEC 27000 – "Information security management systems -- Overview and vocabulary" provides an overview of ISMS, and terms and definitions commonly used in the ISMS family of standards. To ensure consistency in adopted terminology, all 27000 family of standards rely on the terms and definitions provided in ISO/IEC 27000. This standard provides readers with overall starting point by which they can get introduced to the 27000 family.

- ISO/IEC 27003 – "Information security management systems -- Guidance" provides guidance on the requirements for an ISMS as specified in ISO/IEC 27001, as well as the recommendations, possibilities and permissions in relation to the requirements.

- ISO/IEC 27004 – "Information security management -- Monitoring, measurement, analysis and evaluation" provides guidelines to assist organisations in evaluating the information security performance and the effectiveness of an ISMS in order to fulfil the monitoring, measurement, analysis and evaluation requirements as specified in the ISO/IEC 27001.

- ISO/IEC 27005 – "Information security risk management" provides guidelines for information security risk management. It supports the general concepts specified in ISO/IEC 27001 and is designed to assist the satisfactory implementation of information security based on a risk management approach.

- ISO/IEC 27017 – "Code of practice for information security controls based on ISO/IEC 27002 for cloud services" provides guidelines supporting the implementation of information security controls for cloud service consumers and providers. The selection of appropriate controls and the application of the implementation guidance are based on risk assessment and other requirements for the use of cloud services. The standard is accompanied by ISO/IEC 27018 to cover the wider information security angles of cloud computing in addition to privacy.

- ISO/IEC 27031 – "Guidelines for information and communication technology readiness for business continuity" describes the concepts and principles of information and communications technology (ICT) readiness for business continuity, and provides a framework of methods and processes to identify and specify all aspects for improving an organisation's ICT readiness to ensure business continuity.

- ISO/IEC 27035-1 – "Information security incident management -- Part 1: Principles of incident management" provides basic concepts and phases of information security incident management and combines these concepts with principles in a structured approach to detecting, reporting, assessing and responding to incidents, and applying lessons learnt.

- ISO/IEC 27035-2 – "Information security incident management -- Part 2: Guidelines to plan and prepare for incident response" provides guidelines to plan and prepare for incident response.

- ISO/IEC 27036-4 – "Information security for supplier relationships -- Part 4: Guidelines for security of cloud services" defines guidelines supporting the implementation of ISMS for the use of cloud services.

- ISO/IEC 27037 – "Guidelines for identification, collection, acquisition and preservation of digital evidence" provides guidelines for specific activities in the handling of digital evidence, which are identification, collection, acquisition and preservation of potential digital evidence that can be of evidential value.

Personally Identifiable Information (PII) in Cloud Computing

Cloud computing is now evolving like never before. This trend will continue to grow and develop in the coming few years. It is well-known that cloud computing has potential advantages. It is the cost efficient method to use, maintain and upgrade. Backup and recovery method in cloud computing is relatively easier than traditional methods of data storage. Moreover, it gives the advantage of quick deployment and easy access to information.

Some organisations are migrating applications to the cloud. From the organisations' perspective, cloud computing security is of great concern, especially on data security and privacy protection issues, and remains the primary inhibitor for adoption of cloud computing services.

The ISO/IEC 27018:2019 (hereafter referred to as ISO/IEC 27018) standard is known as "Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors". It is the first international standard focusing on the protection of personal data in the public cloud. ISO/IEC 27018 primarily sets forth commonly accepted control objectives, controls and guidelines pertaining to the protection of PII that is processed by the public cloud service providers (i.e., PII processors).

ISO/IEC 27018 has been designed for all types and sizes of organisations in private and public sector providing information processing services via cloud as PII processors.

PII Protection Controls of ISO/IEC 27018

ISO/IEC 27018 was developed taking into account the requirements already contained in ISO/IEC 27002. It augments ISO/IEC 27002 in two approaches: firstly, supplementing implementation guidance for those controls prescribed by ISO/IEC 27002; and, secondly, providing additional controls and associated guidance that are tailored to address public cloud PII protection requirements but not covered by the ISO/IEC 27002 control set. For the first approach, ISO/IEC 27018 provides additional implementation guidance on the following 11 ISO/IEC 27002 controls:

- Information security policies
- Organization of information security
- Human resource security
- Access control
- Cryptography
- Physical and environmental security
- Operations security
- Communications security
- Information security incident management
- Information security aspects of business continuity management
- Compliance

For the second approach, Annex A of ISO/IEC 27018 lists 11 extended ISO/IEC 27002 controls to meet the requirements for PII protection which apply to public cloud service providers acting as PII processors. These extended controls are classified under the 11 privacy principles in ISO/IEC 29100:2011 (hereafter referred to as ISO/IEC 29100), known as "Information technology — Security techniques — Privacy framework". The privacy principles of ISO/IEC 29100 are provided in Appendix A.

Benefits of ISO/IEC 27018

ISO/IEC 27018 is applicable to the processing of PII obtained from a customer for the purposes determined by the customer under its contract with the cloud service provider.

By adopting ISO/IEC 27018, an organisation can:

- Use it as a guideline to facilitate the compliance with the relevant data protection requirements;
- Win the confidence of customers to entrust their data in the cloud, and thus broaden their customer base; and
- Assist public cloud service provider, operating in a multinational market, in coping with various national data protection standards and performing complex assessments in each jurisdiction.

Afterword

ISO/IEC 27001 lays out a formal specification for ISMS, with the emphasis very much on "management system" rather than "information security". A certified ISMS provides a strong indication that an organisation is using a systematic approach for the identification, assessment and management of information security risks. If there is an effective ISMS in operation, then the ISMS will ensure that there are adequate security controls in place. The ISO/IEC 27001 certificate has marketing potential and should help improve credibility and enhance customer confidence.

Appendix A

Table of contents of ISO/IEC 27001:2013

0. Introduction
1. Scope
2. Normative references
3. Terms and definitions
4. Context of the organization
5. Leadership
6. Planning
7. Support
8. Operation
9. Performance evaluation
10. Improvement

Annex A Reference control objectives and controls

Bibliography

The privacy principles of ISO/IEC 29100:2011

1. Consent and choice
2. Purpose legitimacy and specification
3. Collection limitation
4. Data minimization
5. Use, retention and disclosure limitation
6. Accuracy and quality
7. Openness, transparency and notice
8. Individual participation and access
9. Accountability
10. Information security
11. Privacy compliance

Table of contents of ISO/IEC 27002:2013

0. Introduction
1. Scope
2. Normative references
3. Terms and definitions
4. Structure of this standard
5. Information security policies
6. Organization of information security
7. Human resource security
8. Asset management
9. Access control
10. Cryptography
11. Physical and environmental security
12. Operations security
13. Communications security
14. System acquisition, development and maintenance
15. Supplier relationships
16. Information security incident management
17. Information security aspects of business continuity management
18. Compliance

Bibliography

Appendix B

The following ISO/IEC 27000-series information security standards are either published or currently being developed (Note: TR refers to Technical Report; TS refers to Technical Specification):

Standard	Published	Title
ISO/IEC 27000	2018	Information security management systems -- Overview and vocabulary
ISO/IEC 27001	2013	Information security management systems -- Requirements
ISO/IEC 27002	2013*	Code of practice for information security controls
ISO/IEC 27003	2017	Information security management systems -- Guidance
ISO/IEC 27004	2016	Information security management -- Monitoring, measurement, analysis and evaluation
ISO/IEC 27005	2018*	Information security risk management
ISO/IEC 27006	2015*	Requirements for bodies providing audit and certification of information security management systems
ISO/IEC 27007	2020	Guidelines for information security management systems auditing
ISO/IEC TS 27008	2019	Guidelines for the assessment of information security controls
ISO/IEC 27009	2020	Sector-specific application of ISO/IEC 27001 -- Requirements
ISO/IEC 27010	2015*	Information security management for inter-sector and inter-organizational communications
ISO/IEC 27011	2016*	Code of practice for Information security controls based on ISO/IEC 27002 for telecommunications organizations
ISO/IEC 27013	2015*	Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1
ISO/IEC 27014	2013*	Governance of information security
ISO/IEC TR 27016	2014	Information security management -- Organizational economics
ISO/IEC 27017	2015*	Code of practice for information security controls based on ISO/IEC 27002 for cloud services
ISO/IEC 27018	2019	Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors
ISO/IEC 27019	2017	Information security controls for the energy utility industry
ISO/IEC 27021	2017	Competence requirements for information security management systems professionals
ISO/IEC 27022	Draft^	Guidance on information security management system processes
ISO/IEC TR 27023	2015	Mapping the revised editions of ISO/IEC 27001 and ISO/IEC 27002
ISO/IEC 27031	2011*	Guidelines for information and communication technology readiness for business continuity
ISO/IEC 27032	2012*	Guidelines for cybersecurity
ISO/IEC 27033-1	2015*	Network security -- Part 1: Overview and concepts
ISO/IEC 27033-2	2012	Network security -- Part 2: Guidelines for the design and implementation of network security
ISO/IEC 27033-3	2010	Network security -- Part 3: Reference networking scenarios -- Threats, design techniques and control issues
ISO/IEC 27033-4	2014*	Network security -- Part 4: Securing communications between networks using security gateways
ISO/IEC 27033-5	2013	Network security -- Part 5: Securing communications across networks using Virtual Private Networks (VPNs)

Standard	Published	Title
ISO/IEC 27033-6	2016	Network security -- Part 6: Securing wireless IP network access
ISO/IEC 27034-1	2011	Application security -- Part 1: Overview and concepts
ISO/IEC 27034-2	2015*	Application security -- Part 2: Organization normative framework
ISO/IEC 27034-3	2018	Application security -- Part 3: Application security management process
ISO/IEC 27034-4	Draft^	Application security -- Part 4: Validation and verification
ISO/IEC 27034-5	2017	Application security -- Part 5: Protocols and application security controls data structure
ISO/IEC TS 27034-5-1	2018	Application security -- Part 5-1: Protocols and application security controls data structure, XML schemas
ISO/IEC 27034-6	2016	Application security -- Part 6: Case studies
ISO/IEC 27034-7	2018	Application security -- Part 7: Assurance prediction framework
ISO/IEC 27035-1	2016*	Information security incident management -- Part 1: Principles of incident management
ISO/IEC 27035-2	2016*	Information security incident management -- Part 2: Guidelines to plan and prepare for incident response
ISO/IEC 27035-3	2020	Information security incident management -- Part 3: Guidelines for ICT incident response operations
ISO/IEC 27035-4	Draft^	Information security incident management - Part 4: Coordination
ISO/IEC 27036-1	2014	Information security for supplier relationships -- Part 1: Overview and concepts
ISO/IEC 27036-2	2014	Information security for supplier relationships -- Part 2: Requirements
ISO/IEC 27036-3	2013	Information security for supplier relationships -- Part 3: Guidelines for information and communication technology supply chain security
ISO/IEC 27036-4	2016	Information security for supplier relationships -- Part 4: Guidelines for security of cloud services
ISO/IEC 27037	2012	Guidelines for identification, collection, acquisition and preservation of digital evidence
ISO/IEC 27038	2014	Specification for digital redaction
ISO/IEC 27039	2015	Selection, deployment and operations of intrusion detection and prevention systems (IDPS)
ISO/IEC 27040	2015*	Storage security
ISO/IEC 27041	2015*	Guidance on assuring suitability and adequacy of incident investigative method
ISO/IEC 27042	2015*	Guidelines for the analysis and interpretation of digital evidence
ISO/IEC 27043	2015	Incident investigation principles and processes
ISO/IEC 27045	Draft^	Big data security and privacy -- Processes
ISO/IEC 27046	Draft^	Big data security and privacy -- Implementation guidelines
ISO/IEC 27050-1	2019	Electronic discovery -- Part 1: Overview and concepts
ISO/IEC 27050-2	2018	Electronic discovery -- Part 2: Guidance for governance and management of electronic discovery
ISO/IEC 27050-3	2020	Electronic discovery -- Part 3: Code of practice for electronic discovery
ISO/IEC 27050-4	Draft^	Electronic discovery -- Part 4: Technical readiness
ISO/IEC 27070	Draft^	Requirements for establishing virtualized roots of trust
ISO/IEC 27071	Draft^	Security recommendations for establishing trusted connection between devices and services
ISO/IEC 27099	Draft^	Public key infrastructure -- Practices and policy framework

An Overview of ISO/IEC 27000 family of Information Security Management System Standards

Standard	Published	Title
ISO/IEC TS 27100	Draft^	Cybersecurity -- Overview and concepts
ISO/IEC 27102	2019	Guidelines for cyber-insurance
ISO/IEC TR 27103	2018	Cybersecurity and ISO and IEC Standards
ISO/IEC 27110	Draft^	Cybersecurity framework development guidelines
ISO/IEC 27400	Draft^	IoT security and privacy -- Guidelines
ISO/IEC 27402	Draft^	IoT security and privacy -- Device baseline requirements
ISO/IEC 27403	Draft^	IoT security and privacy -- Guidelines for IoT-domotics
ISO/IEC TR 27550	2019	Privacy engineering for system life cycle processes
ISO/IEC 27551	Draft^	Requirements for attribute-based unlinkable entity authentication
ISO/IEC 27553	Draft^	Security requirements for authentication using biometrics on mobile devices
ISO/IEC 27554	Draft^	Application of ISO 31000 for assessment of identity management-related risk
ISO/IEC 27555	Draft^	Guidelines on personally identifiable information deletion
ISO/IEC 27556	Draft^	User-centric framework for the handling of personally identifiable information (PII) based on privacy preferences
ISO/IEC 27557	Draft^	Organizational privacy risk management
ISO/IEC 27559	Draft^	Privacy enhancing data de-identification framework
ISO/IEC 27560	Draft^	Privacy technologies -- Consent record information structure
ISO/IEC TS 27570	Draft^	Privacy guidelines for Smart Cities
ISO/IEC 27701	2019	Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management -- Requirements and guidelines
ISO 27799 #	2016	Health informatics -- Information security management in health using ISO/IEC 27002

^ Under development; * Under revision;
# International Standards not under the same general title that are also part of the ISO/IEC 27000 family of standards

References

1. Refer to https://www.iso.org
   on the contents of ISO/IEC 27000 Family
2. Refer to http://www.pc-history.org/17799.htm
   on the history of ISO/IEC 27001
3. Refer to https://www.iso.org/the-iso-survey.html
   on ISO certificate survey