

Kybernetická bezpečnosť v meniacich sa podmienkach (odborný seminár)

Bratislava, 20.9.2023

Rozdiely medzi všeobecným riadením rizík (ISO 31001) a špecifickým rizík informačnej bezpečnosti (ISO 27005)

Autor(i): Róbert Kormaňák

Zástupca SR pre štandardizáciu ISO v oblasti softvérového inžinierstva, IT služieb, kvality, riadenia rizík a riadenia projektov

Keywords:

- Risk • Risk Management • Standard • Standardisation • ISO • National Standards • International Standards • Standard Evolution •
- Information Security • Cyber-security • Information Assets • Information Threats • Information Vulnerability •

Agenda

1. Basic Terms and Definitions
2. Standardisation and ISO
3. Evolution of ISO 31000
4. Evolution of ISO 27000
5. Evolution of ISO 27005
6. Risk Management by ISO 31000
7. Risk Management by ISO 27005
8. Summary

1. Basic Terms and Definitions

Pôvod termínu Risk je možné odvodiť z klasickej gréčtiny – od slova **ρίζα**, čo znamená **koreň**

- V gréčtine navigačný termín **rhizikon, rhiza**, ktorý významovo znamenal “koreň, skala, pevná pôda” a slúžil ako metafora pre “prekážky na mori, ktorým sa treba vyhnúť”.
- V latinčine a vulgárnej latinčine **resicum, risicum, riscus** vo význame útes
- V taliančine **risco, riscio** (súčasný **rischio**) odvodené od **risicare** „ide do nebezpečenstva”



1. Basic Terms and Definitions



1. Basic Terms and Definitions

ISO 31000:2018

3.1 risk

effect of uncertainty on objectives

Note 1 to entry: An effect is a deviation from the expected. It can be positive, negative or both. An effect can arise as a result of a response, or failure to respond, to an opportunity or to a threat related to objectives.

Note 2 to entry: Objectives can have different aspects and categories, and can be applied at different levels.

Note 3 to entry: Risk is usually expressed in terms of *risk sources* ([3.4](#)), potential *events* ([3.5](#)), their *consequences* ([3.6](#)) and their *likelihood* ([3.7](#)).

[SOURCE: ISO Guide 73:2009, 1.1, modified — The original five Notes to entry have been modified and combined into three Notes to entry]

ISO 31000:2018

3.2 risk management

coordinated activities to direct and control an organization with regard to *risk* ([3.1](#))

[SOURCE: ISO Guide 73:2009, 2.1]

1. Basic Terms and Definitions

ISO 31000:2018

3.4

risk source

element which alone or in combination has the potential to give rise to *risk* ([3.1](#))

[SOURCE: ISO Guide 73:2009, 3.5.1.2, modified — The word “intrinsic” has been deleted before “potential” and the original Note to entry has been deleted]

ISO 31000:2018

3.5

event

occurrence or change of a particular set of circumstances

Note 1 to entry: An event can be one or more occurrences, and can have several causes and several *consequences* ([3.6](#)).

Note 2 to entry: An event can also be something that is expected which does not happen, or something that is not expected which does happen.

Note 3 to entry: An event can be a risk source.

[SOURCE: ISO Guide 73:2009, 3.5.1.3, modified — The original four Notes to entry have been modified and combined into three Notes to entry]

1. Basic Terms and Definitions

ISO 31000:2018

3.6

consequence

outcome of an *event* (3.5) affecting objectives

Note 1 to entry: A consequence can be certain or uncertain and can have positive or negative direct or indirect effects on objectives.

Note 2 to entry: Consequences can be expressed qualitatively or quantitatively.

Note 3 to entry: Initial consequences can escalate through cascading and cumulative effects.

[SOURCE: ISO Guide 73:2009, 3.6.1.3, modified — The original four Notes to entry have been modified and combined into three Notes to entry]

ISO 31000:2018

3.7

likelihood

chance of something happening

Note 1 to entry: In *risk management* (3.2) terminology, the word “likelihood” is used to refer to the chance of something happening, whether defined, measured or determined objectively or subjectively, qualitatively or quantitatively, and described using general terms or mathematically (such as a probability or a frequency over a given time period).

Note 2 to entry: The English term “likelihood” does not have a direct equivalent in some languages; instead, the equivalent of the term “probability” is often used. However, in English, “probability” is often narrowly interpreted as a mathematical term. Therefore, in risk management terminology, “likelihood” is used with the intent that it should have the same broad interpretation as the term “probability” has in many languages other than English.

[SOURCE: ISO Guide 73:2009, 3.6.1.1]

1. Basic Terms and Definitions

ISO 27005:2022

3.1.5

risk owner

person or entity with the accountability and authority to manage a *risk* ([3.1.3](#))

[SOURCE: ISO Guide 73:2009, 3.5.1.5]

ISO 27005:2022

3.1.6

risk source

element which alone or in combination has the potential to give rise to *risk* ([3.1.3](#))

Note 1 to entry: A risk source can be one of these three types:

- human;
- environmental;
- technical.

Note 2 to entry: A human risk source type can be intentional or unintentional.

[SOURCE: ISO 31000:2018, 3.4, modified—Notes 1 and 2 to entry have been added.]

ISO 27005:2022

3.1.7

risk criteria

terms of reference against which the significance of a *risk* ([3.1.3](#)) is evaluated

Note 1 to entry: Risk criteria are based on organizational objectives, and *external context* ([3.1.1](#)) and *internal context* ([3.1.2](#)).

Note 2 to entry: Risk criteria can be derived from standards, laws, policies and other requirements.

[SOURCE: ISO Guide 73:2009, 3.3.1.3]

1. Basic Terms and Definitions

ISO 27005:2022

3.1.9

threat

potential cause of an *information security incident* ([3.1.12](#)) that can result in damage to a system or harm to an organization

ISO 27005:2022

3.1.10

vulnerability

weakness of an asset or *control* ([3.1.16](#)) that can be exploited so that an *event* ([3.1.11](#)) with a negative *consequence* ([3.1.14](#)) occurs

ISO 27005:2022

3.1.11

event

occurrence or change of a particular set of circumstances

Note 1 to entry: An event can have one or more occurrences, and can have several causes and several *consequences* ([3.1.14](#)).

Note 2 to entry: An event can also be something that is expected which does not happen, or something that is not expected which does happen.

[SOURCE: ISO 31000:2018, 3.5, modified—Note 3 to entry has been removed.]

1. Basic Terms and Definitions

ISO 27005:2022

3.2.7

risk treatment

process to modify *risk* ([3.1.3](#))

Note 1 to entry: Risk treatment can involve:

- avoiding the risk by deciding not to start or continue with the activity that gives rise to the risk;
- taking or increasing risk in order to pursue an opportunity;
- removing the *risk source* ([3.1.6](#));
- changing the *likelihood* ([3.1.13](#));
- changing the *consequences* ([3.1.14](#));
- sharing the *risk* ([3.1.3](#)) with another party or parties (including contracts and risk financing); and
- retaining the *risk* ([3.1.3](#)) by informed decision.

Note 2 to entry: Information security risk treatment does not include “taking or increasing risk in order to pursue an opportunity” but the organization can have this option for general risk management.

Note 3 to entry: Risk treatments that deal with negative consequences are sometimes referred to as “risk mitigation”, “risk elimination”, “risk prevention” and “risk reduction”.

Note 4 to entry: Risk treatment can create new risks or modify existing risks.

[SOURCE: ISO Guide 73:2009, 3.8.1, modified — Note 1 to entry has been added and the original Note 1 and 2 to entry have been renumbered as Note 2 and 3 to entry.]

1. Basic Terms and Definitions

ISO 27005:2022

3.2.8

risk acceptance

informed decision to take a particular *risk* ([3.1.3](#))

Note 1 to entry: Risk acceptance can occur without *risk treatment* ([3.2.7](#)) or during the process of risk treatment.

Note 2 to entry: Accepted risks are subject to monitoring and review.

[SOURCE: ISO Guide 73:2009, 3.7.1.6]

ISO 27005:2022

3.2.9

risk sharing

form of *risk treatment* ([3.2.7](#)) involving the agreed distribution of *risk* ([3.1.3](#)) with other parties

Note 1 to entry: Legal or regulatory requirements can limit, prohibit or mandate risk sharing.

Note 2 to entry: Risk sharing can be carried out through insurance or other forms of contract.

Note 3 to entry: The extent to which risk is distributed can depend on the reliability and clarity of the sharing arrangements.

Note 4 to entry: Risk transfer is a form of risk sharing.

[SOURCE: ISO Guide 73:2009, 3.8.1.3]

ISO 27005:2022

3.2.10

risk retention

temporary acceptance of the potential benefit of gain, or burden of loss, from a particular *risk* ([3.1.3](#))

Note 1 to entry: **Retention** can be restricted to a certain period of time.

Note 2 to entry: The *level of risk* ([3.1.15](#)) retained can depend on *risk criteria* ([3.1.7](#)).

2. Standardisation and ISO

ISO (International Organization for Standardization) is the world's largest developer of **voluntary** International Standards. International Standards give state of the art specifications for products, services and good practice, helping to make industry more efficient and effective.

The conference of national standardizing organizations which established ISO took place in London from **14 to 26 October, 1946**. 65 delegates from 25 countries meet to discuss the future of International Standardization. In 1947, ISO officially comes into existence with 67 technical committees (groups of experts focusing on a specific subject).

ISO was born from the union of two organisations:

- **ISA (International Federation of the National Standardizing Associations)**, established in New York in 1926, and administered from Switzerland.
- **UNSCC (United Nations Standards Coordinating Committee)**, established only in 1944, and administered in London.



The conference of the national standards bodies at which it was decided to establish ISO took place at the Institute of Civil Engineers in London from 14 to 26 October 1946. Twenty-five countries were represented by 65 delegates.

2. Standardisation and ISO



1960

SI - International System of Units

In 1960, ISO publishes the standard ISO 31 on quantities and units (which has since been replaced by ISO 80 000).

ISO 31 is based on SI (Système international d'unités). The SI sets out one unit for each quantity, for example, the metre for distance and the second for time. The objective of the SI system is to reach world-wide uniformity in units of measurement.

ISO 80 000 sets out these units and how to use them.

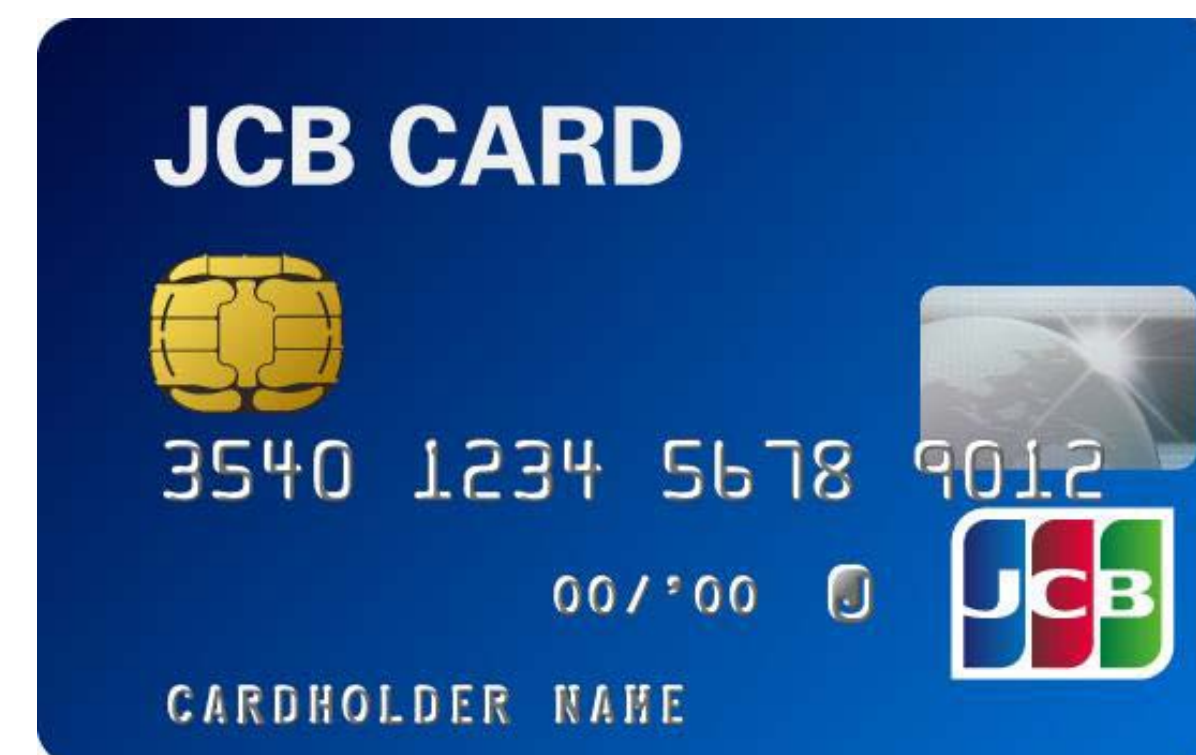
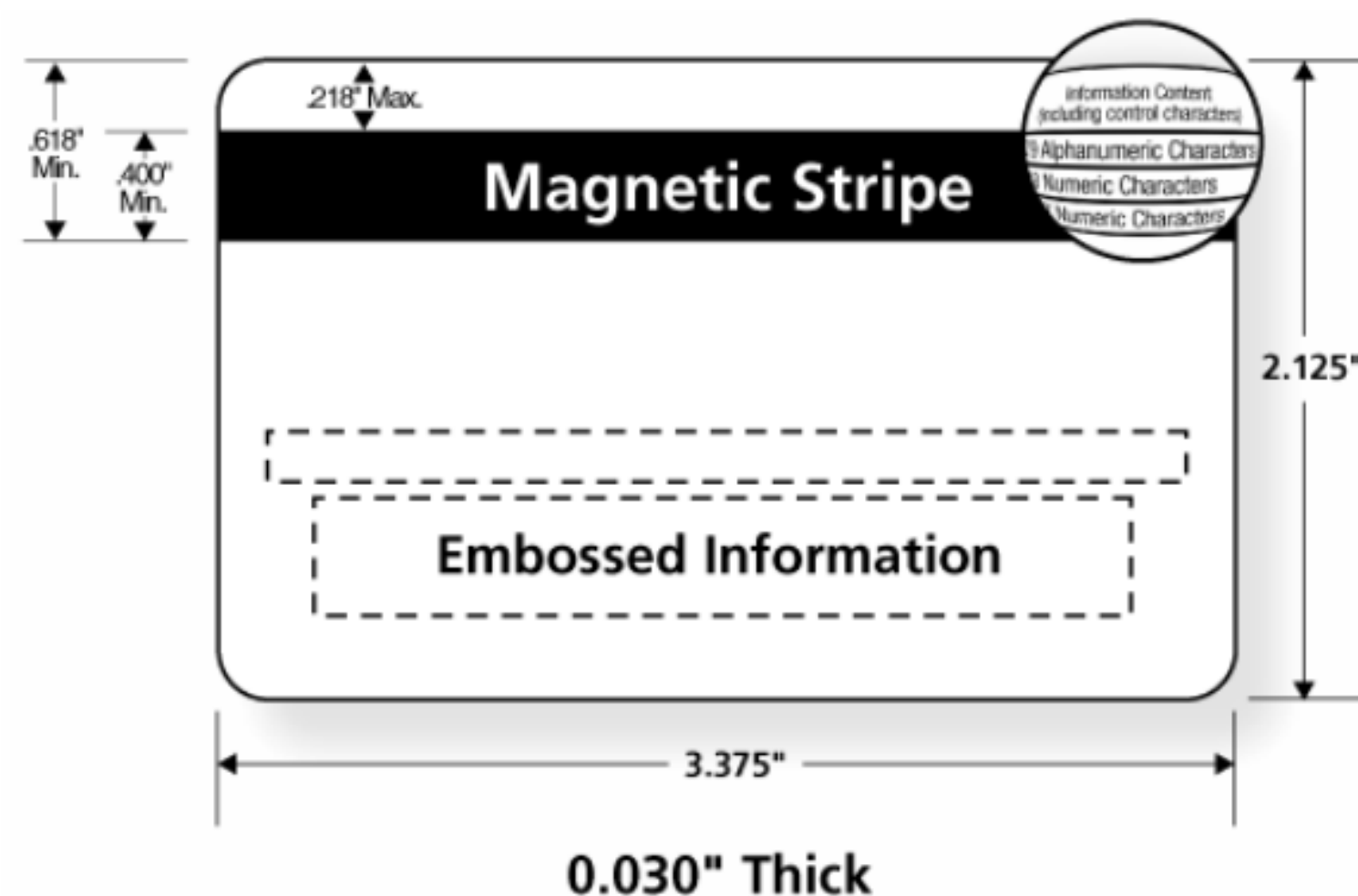
2. Standardisation and ISO



Základom je 20 stopový univerzálny kontajner s uzavretými stenami a čelnými dverami pre nakládku a vykládku od ktorého je odvodená aj základná merná jednotka pre vyjádrenie kapacity a výkonov v kombinovanej doprave TEU - Twenty Equivalent Unit - ekvivalent dvadsaťstopového kontajnera.

2. Standardisation and ISO

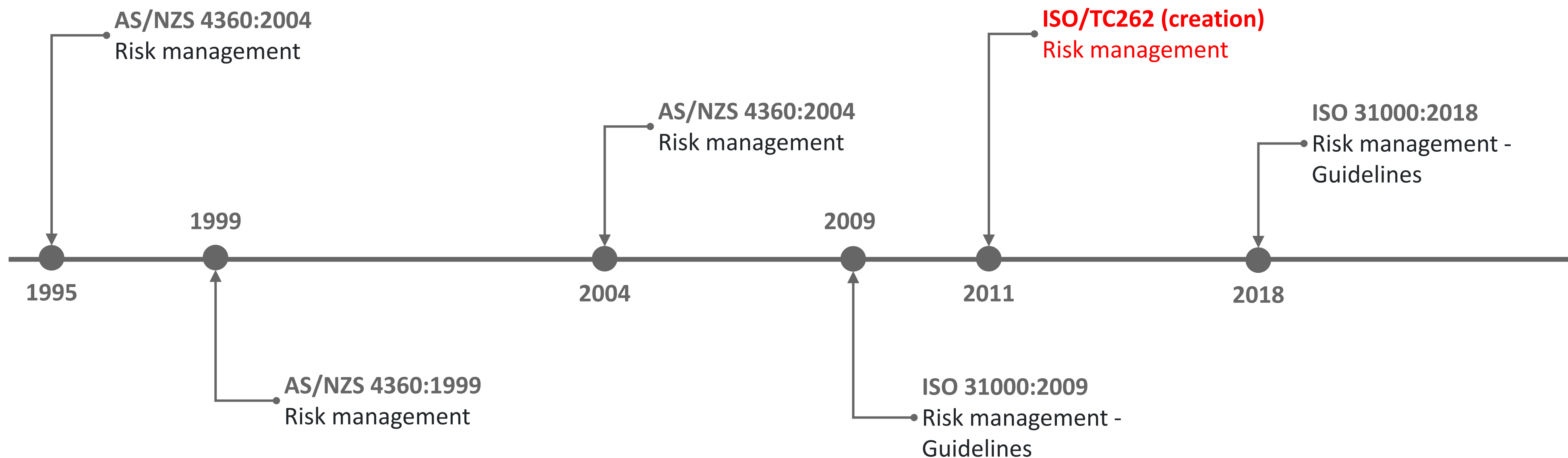
ISO	7810	Identification Cards - Physical Characteristics
	7811-1	Embossing
	7811-2	Magnetic stripe - low coercivity
	7811-3	Location of embossed characters on ID-1 cards
	7811-6	Magnetic stripe - high coercivity
	7813	Financial transaction cards



2. Standardisation and ISO



3. Evolution of ISO 31000



3. Evolution of ISO 31000

← Technical Committees

ISO/TC 262

Risk management

About

Secretariat: **BSI**

Committee Manager: **Mrs Nyomee Hla-Shwe Tun**

Chairperson (until end 2025): Dr Russell Price

ISO Technical Programme Manager [TPM]: **Mr Ben Carson**

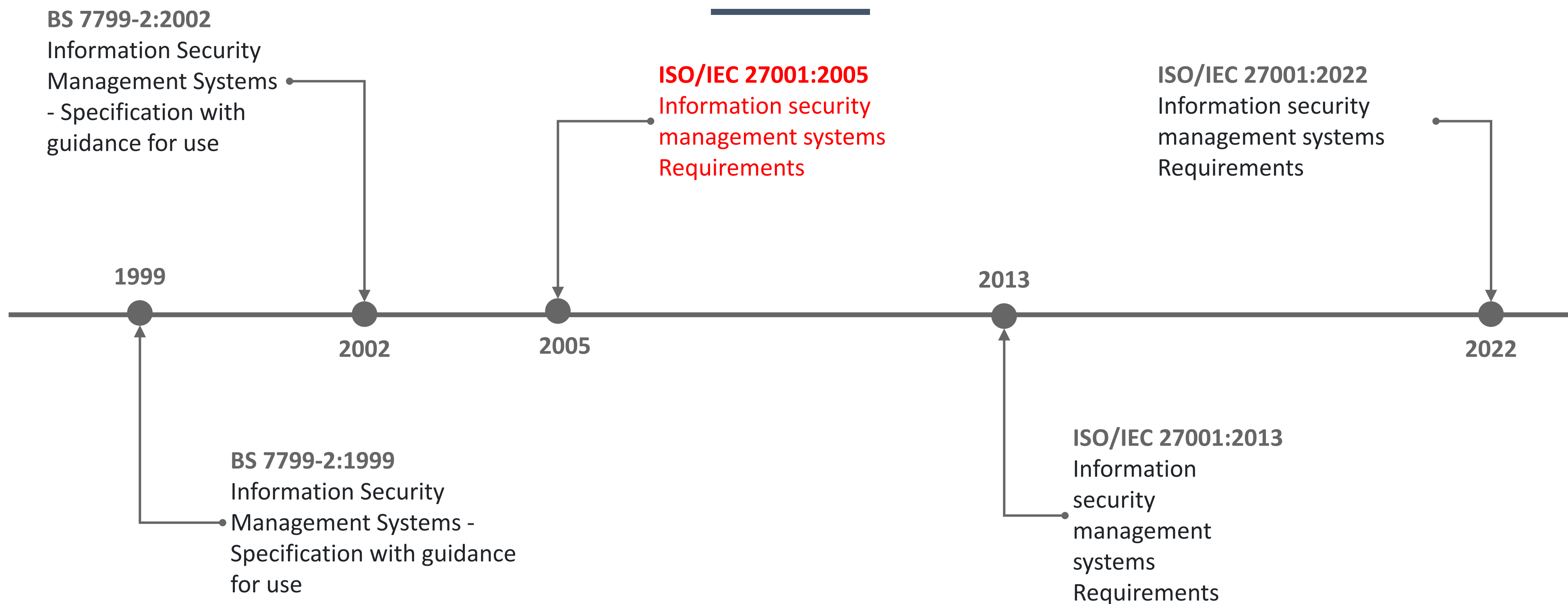
ISO Editorial Manager [EM]: **Ms Sanjali Jain**

Creation date: 2011

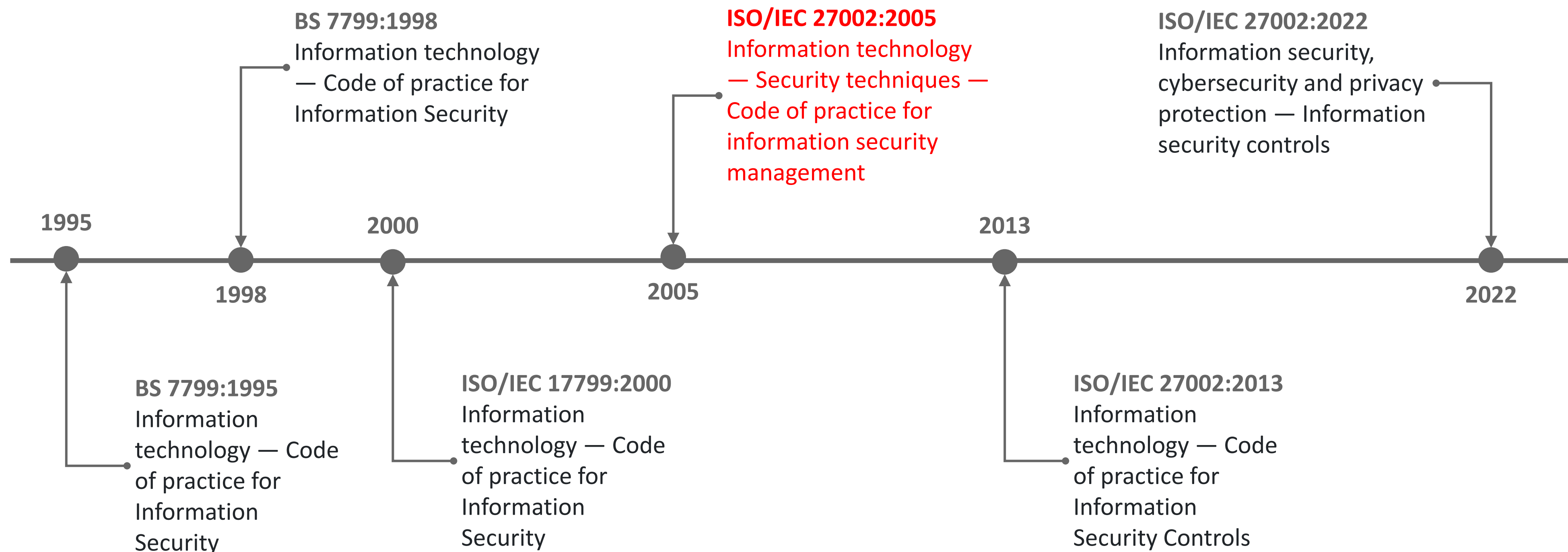
3. Evolution of ISO 31000

Standard and/or project under the direct responsibility of ISO/TC 262 Secretariat ⁽⁶⁾ ↑	Stage	ICS
✓ IWA 31:2020 Risk management — Guidelines on using ISO 31000 in management systems	60.60	03.100.01
✓ ISO 31000:2018 Risk management — Guidelines	90.60	03.100.01
✓ IEC 31010:2019 Risk management — Risk assessment techniques	60.60	03.100.01
✓ ISO 31022:2020 Risk management — Guidelines for the management of legal risk	60.60	03.100.01
✓ ISO 31030:2021 Travel risk management — Guidance for organizations	60.60	03.100.01
✓ ISO 31073:2022 Risk management — Vocabulary	60.60	01.040.03 03.100.01

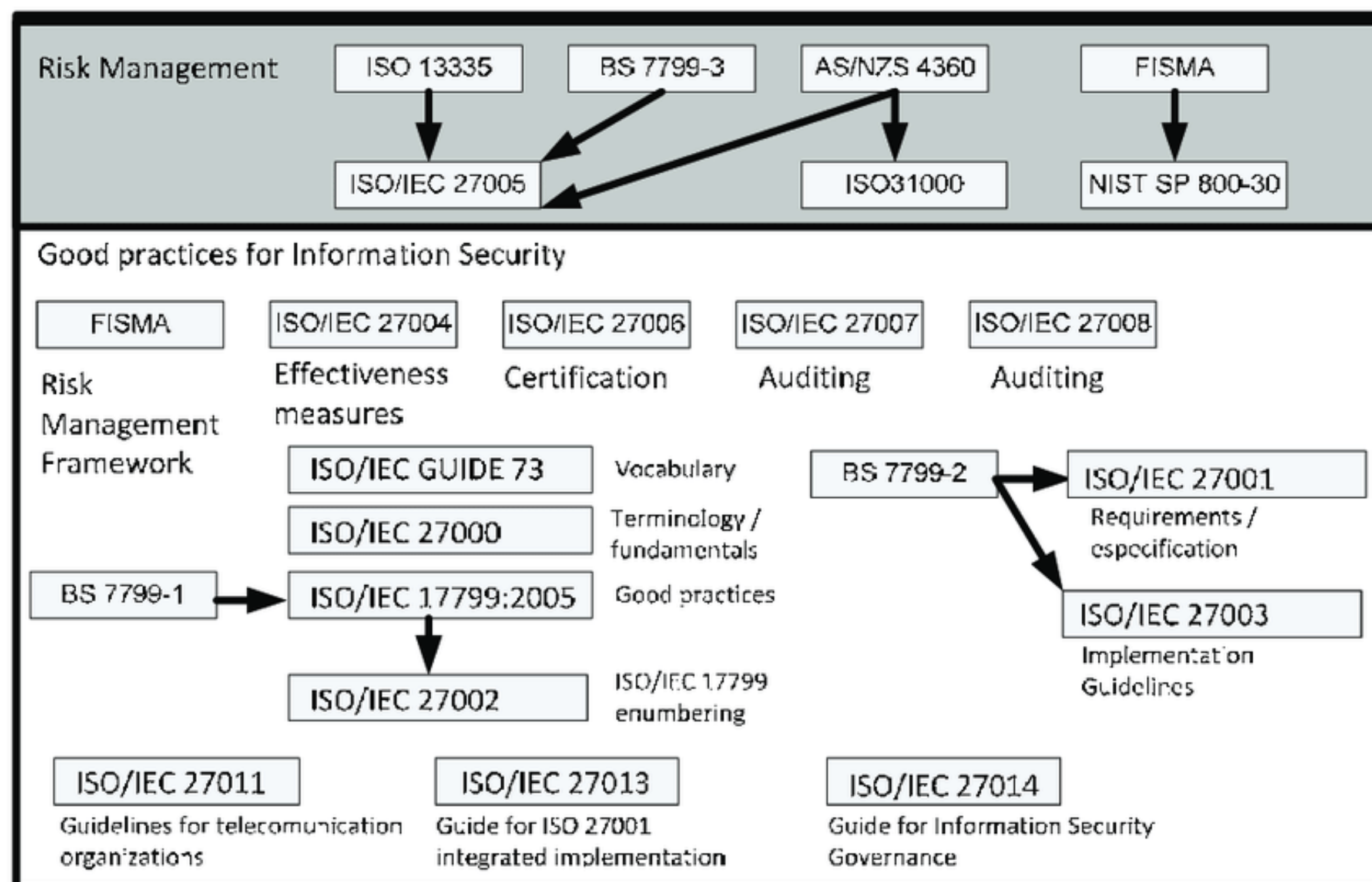
4. Evolution of ISO 27001



4. Evolution of ISO 27002



4. Evolution of ISO 27000 Family



4. Evolution of ISO 27000

← ISO/IEC JTC 1

ISO/IEC JTC 1/SC 27

Information security, cybersecurity and privacy protection

About

Secretariat: **DIN**

Committee Manager: **Mr Sobhi Mahmoud**

Chairperson (until end 2024): Mr Dr Andreas Wolf

ISO Technical Programme Manager [TPM]: **Mr Hakim Mkinsi**

ISO Editorial Manager [EM]: **Ms Isabel Veronica Nelson**

Creation date: 1989

4. Evolution of ISO 27000

Reference ↑	Title	Type
ISO/IEC JTC 1/SC 27/AG 2 ⓘ	Trustworthiness	Working group
ISO/IEC JTC 1/SC 27/AG 5 ⓘ	Strategy	Working group
ISO/IEC JTC 1/SC 27/AG 6 ⓘ	Operations	Working group
ISO/IEC JTC 1/SC 27/AG 7 ⓘ	Communication and Outreach (AG-CO)	Working group
ISO/IEC JTC 1/SC 27/AG 8 ⓘ	Advisory Group on Conformity Assessment	Working group
ISO/IEC JTC 1/SC 27/AHG 1 ⓘ	Resolution Drafting	Working group
ISO/IEC JTC 1/SC 27/AHG 2 ⓘ	Security and privacy in IoT and Digital Twin	Working group
ISO/IEC JTC 1/SC 27/AHG 3 ⓘ	Security and privacy in AI and Big Data (BD)	Working group
ISO/IEC JTC 1/SC 27/CAG ⓘ	Chair's Advisory Group	Working group
ISO/IEC JTC 1/SC 27/JWG 6 ⓘ	Joint ISO/IEC JTC1/SC 27 - ISO/TC 22/SC 32 WG : Cybersecurity requirements and evaluation activities for connected vehicle devices	Working group
ISO/IEC JTC 1/SC 27/WG 1 ⓘ	Information security management systems	Working group
ISO/IEC JTC 1/SC 27/WG 2 ⓘ	Cryptography and security mechanisms	Working group
ISO/IEC JTC 1/SC 27/WG 3 ⓘ	Security evaluation, testing and specification	Working group
ISO/IEC JTC 1/SC 27/WG 4 ⓘ	Security controls and services	Working group
ISO/IEC JTC 1/SC 27/WG 5 ⓘ	Identity management and privacy technologies	Working group

4. Evolution of ISO 27000

SUSTAINABLE
DEVELOPMENT GOALS

This committee contributes with 37 standards to the following Sustainable Development Goals:

3 4 5 8 9 10 11 12 13 16

236

Published ISO standards *

62

ISO standards under
development *

57

Participating members

33

Observing members

4. Evolution of ISO 27000 (a)

✓ ISO/IEC 27000:2018 Information technology — Security techniques — Information security management systems — Overview and vocabulary	90.92	35.030 01.040.35
✓ ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements	60.60	35.030 03.100.70
✓ ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection — Information security controls	60.60	35.030
✓ ISO/IEC 27003:2017 Information technology — Security techniques — Information security management systems — Guidance	90.60	35.030 03.100.70
✓ ISO/IEC 27004:2016 Information technology — Security techniques — Information security management — Monitoring, measurement, analysis and evaluation	90.60	35.030
✓ ISO/IEC 27005:2022 Information security, cybersecurity and privacy protection — Guidance on managing information security risks	60.60	35.030
✓ ISO/IEC TS 27006-2:2021 Requirements for bodies providing audit and certification of information security management systems — Part 2: Privacy information management systems	90.92	35.030 03.120.20
✓ ISO/IEC 27006:2015 Information technology — Security techniques — Requirements for bodies providing audit and certification of information security management systems	90.92	35.030 03.120.20
✓ ISO/IEC 27006:2015/Amd 1:2020 Information technology — Security techniques — Requirements for bodies providing audit and certification of information security management systems — Amendment 1	60.60	35.030

4. Evolution of ISO 27000 (b)

ISO/IEC 27007:2020 Information security, cybersecurity and privacy protection — Guidelines for information security management systems auditing	60.60	35.030 03.120.20
ISO/IEC TS 27008:2019 Information technology — Security techniques — Guidelines for the assessment of information security controls	90.60	35.030
ISO/IEC 27010:2015 Information technology — Security techniques — Information security management for inter-sector and inter-organizational communications	90.93	35.030 03.100.70
ISO/IEC 27011:2016 Information technology — Security techniques — Code of practice for Information security controls based on ISO/IEC 27002 for telecommunications organizations	90.92	35.030
ISO/IEC 27011:2016/Cor 1:2018 Information technology — Security techniques — Code of practice for Information security controls based on ISO/IEC 27002 for telecommunications organizations — Technical Corrigendum 1	60.60	35.030
ISO/IEC 27013:2021 Information security, cybersecurity and privacy protection — Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1	60.60	35.020 35.030 03.080.99 03.100.70
ISO/IEC 27014:2020 Information security, cybersecurity and privacy protection — Governance of information security	60.60	35.030

4. Evolution of ISO 27000 (c)

✓ ISO/IEC TR 27016:2014 Information technology — Security techniques — Information security management — Organizational economics	60.60	35.030
✓ ISO/IEC 27017:2015 Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services	90.92	35.030
✓ ISO/IEC 27018:2019 Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors	60.60	35.030
✓ ISO/IEC 27019:2017 Information technology — Security techniques — Information security controls for the energy utility industry	90.92	35.030
✓ ISO/IEC 27021:2017 Information technology — Security techniques — Competence requirements for information security management systems professionals	90.60	35.030
✓ ISO/IEC 27021:2017/Amd 1:2021 Information technology — Security techniques — Competence requirements for information security management systems professionals — Amendment 1: Addition of ISO/IEC 27001:2013 clauses or subclauses to competence requirements	60.60	35.030
✓ ISO/IEC TS 27022:2021 Information technology — Guidance on information security management system processes	60.60	35.030 03.100.70

4. Evolution of ISO 27000 (d)

✓ ISO/IEC 27031:2011 Information technology — Security techniques — Guidelines for information and communication technology readiness for business continuity	90.92	35.030
✓ ISO/IEC 27032:2023 Cybersecurity — Guidelines for Internet security	60.60	35.030
✓ ISO/IEC 27033-1:2015 Information technology — Security techniques — Network security — Part 1: Overview and concepts	90.93	35.030
✓ ISO/IEC 27033-2:2012 Information technology — Security techniques — Network security — Part 2: Guidelines for the design and implementation of network security	90.20	35.030
✓ ISO/IEC 27033-3:2010 Information technology — Security techniques — Network security — Part 3: Reference networking scenarios — Threats, design techniques and control issues	90.93	35.030
✓ ISO/IEC 27033-4:2014 Information technology — Security techniques — Network security — Part 4: Securing communications between networks using security gateways	90.93	35.030
✓ ISO/IEC 27033-5:2013 Information technology — Security techniques — Network security — Part 5: Securing communications across networks using Virtual Private Networks (VPNs)	90.93	35.030
✓ ISO/IEC 27033-6:2016 Information technology — Security techniques — Network security — Part 6: Securing wireless IP network access	90.93	35.030

4. Evolution of ISO 27000 (e)

✓ ISO/IEC 27034-1:2011 Information technology — Security techniques — Application security — Part 1: Overview and concepts	90.93	35.030
✓ ISO/IEC 27034-1:2011/Cor 1:2014 Information technology — Security techniques — Application security — Part 1: Overview and concepts — Technical Corrigendum 1	60.60	35.030
✓ ISO/IEC 27034-2:2015 Information technology — Security techniques — Application security — Part 2: Organization normative framework	90.93	35.030
✓ ISO/IEC 27034-3:2018 Information technology — Application security — Part 3: Application security management process	90.60	35.030
✓ ISO/IEC 27034-5:2017 Information technology — Security techniques — Application security — Part 5: Protocols and application security controls data structure	90.93	35.030
✓ ISO/IEC 27034-6:2016 Information technology — Security techniques — Application security — Part 6: Case studies	90.93	35.030
✓ ISO/IEC 27034-7:2018 Information technology — Application security — Part 7: Assurance prediction framework	90.60	35.030

4. Evolution of ISO 27000 (f)

✓ ISO/IEC TS 27034-5-1:2018 Information technology — Application security — Part 5-1: Protocols and application security controls data structure, XML schemas	90.93	35.030
✓ ISO/IEC 27035-1:2023 Information technology — Information security incident management — Part 1: Principles and process	60.60	35.030
✓ ISO/IEC 27035-2:2023 Information technology — Information security incident management — Part 2: Guidelines to plan and prepare for incident response	60.60	35.030
✓ ISO/IEC 27035-3:2020 Information technology — Information security incident management — Part 3: Guidelines for ICT incident response operations	60.60	35.030
✓ ISO/IEC 27036-1:2021 Cybersecurity — Supplier relationships — Part 1: Overview and concepts	60.60	35.030
✓ ISO/IEC 27036-2:2022 Cybersecurity — Supplier relationships — Part 2: Requirements	60.60	35.030
✓ ISO/IEC 27036-3:2023 Cybersecurity — Supplier relationships — Part 3: Guidelines for hardware, software, and services supply chain security	60.60	35.030
✓ ISO/IEC 27036-4:2016 Information technology — Security techniques — Information security for supplier relationships — Part 4: Guidelines for security of cloud services	90.93	35.030

4. Evolution of ISO 27000 (g)

ISO/IEC 27037:2012 Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence	90.20	35.030
ISO/IEC 27038:2014 Information technology — Security techniques — Specification for digital redaction	90.93	35.030
ISO/IEC 27039:2015 Information technology — Security techniques — Selection, deployment and operations of intrusion detection and prevention systems (IDPS)	90.93	35.030
ISO/IEC 27040:2015 Information technology — Security techniques — Storage security	90.92	35.030
ISO/IEC 27041:2015 Information technology — Security techniques — Guidance on assuring suitability and adequacy of incident investigative method	90.93	35.030
ISO/IEC 27042:2015 Information technology — Security techniques — Guidelines for the analysis and interpretation of digital evidence	90.93	35.030
ISO/IEC 27043:2015 Information technology — Security techniques — Incident investigation principles and processes	90.93	35.030
ISO/IEC 27050-1:2019 Information technology — Electronic discovery — Part 1: Overview and concepts	60.60	35.030
ISO/IEC 27050-2:2018 Information technology — Electronic discovery — Part 2: Guidance for governance and management of electronic discovery	60.60	35.030

4. Evolution of ISO 27000 (h)

✓ ISO/IEC 27050-3:2020 Information technology — Electronic discovery — Part 3: Code of practice for electronic discovery	60.60	35.030
✓ ISO/IEC 27050-4:2021 Information technology — Electronic discovery — Part 4: Technical readiness	60.60	35.030
✓ ISO/IEC 27070:2021 Information technology — Security techniques — Requirements for establishing virtualized roots of trust	60.60	35.030
✓ ISO/IEC 27071:2023 Cybersecurity — Security recommendations for establishing trusted connections between devices and services	60.60	35.030
✓ ISO/IEC 27099:2022 Information technology — Public key infrastructure — Practices and policy framework	60.60	35.030
✓ ISO/IEC TS 27100:2020 Information technology — Cybersecurity — Overview and concepts	60.60	35.030
✓ ISO/IEC 27102:2019 Information security management — Guidelines for cyber-insurance	60.60	35.030
✓ ISO/IEC TR 27103:2018 Information technology — Security techniques — Cybersecurity and ISO and IEC Standards	90.92	35.030

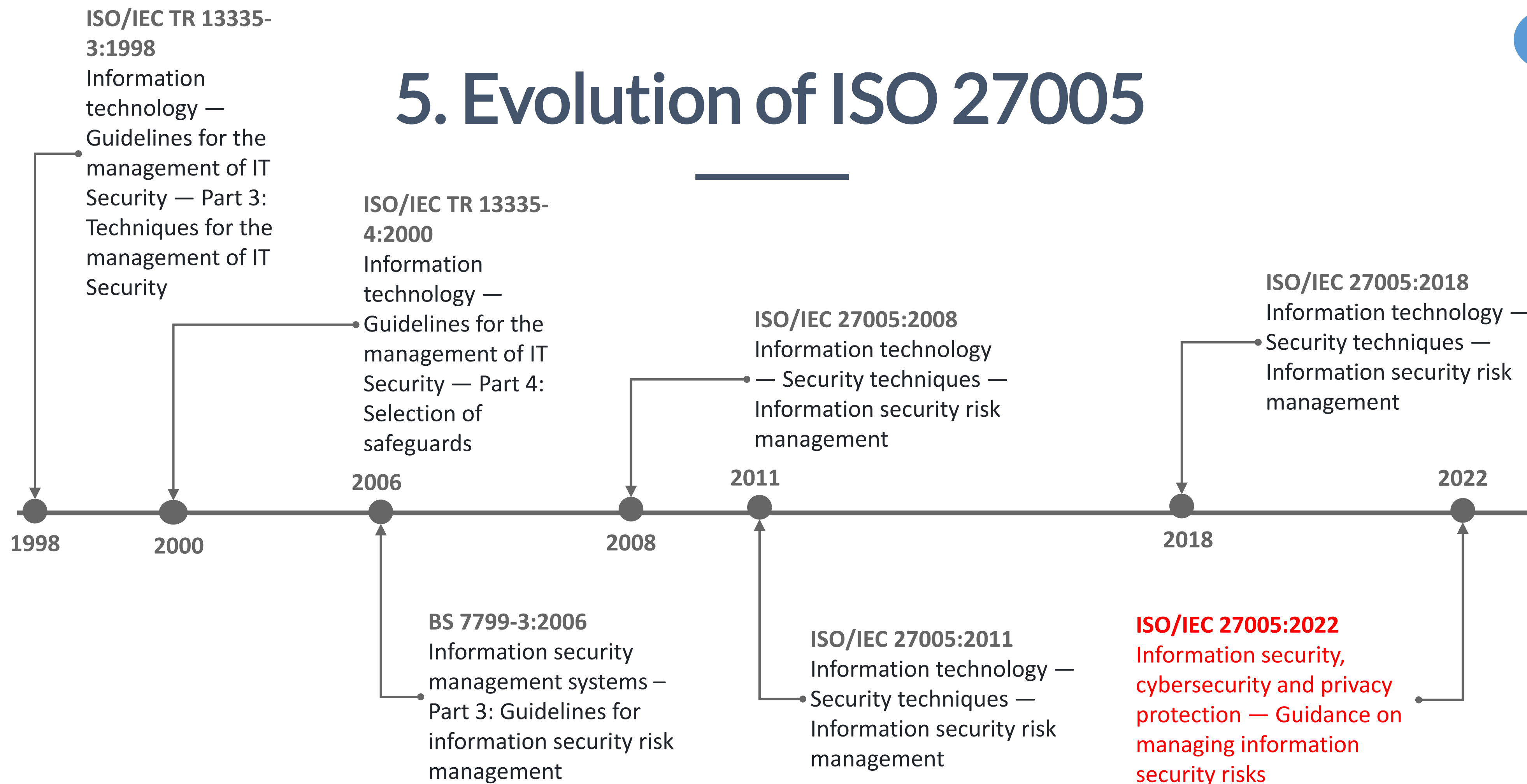
4. Evolution of ISO 27000 (i)

✓ ISO/IEC TS 27110:2021 Information technology, cybersecurity and privacy protection — Cybersecurity framework development guidelines	60.60	35.030
✓ ISO/IEC 27400:2022 Cybersecurity — IoT security and privacy — Guidelines	60.60	35.030
✓ ISO/IEC TR 27550:2019 Information technology — Security techniques — Privacy engineering for system life cycle processes	60.60	35.030
✓ ISO/IEC 27551:2021 Information security, cybersecurity and privacy protection — Requirements for attribute-based unlinkable entity authentication	60.60	35.030
✓ ISO/IEC 27553-1:2022 Information security, cybersecurity and privacy protection — Security and privacy requirements for authentication using biometrics on mobile devices — Part 1: Local modes	60.60	35.030
✓ ISO/IEC 27555:2021 Information security, cybersecurity and privacy protection — Guidelines on personally identifiable information deletion	60.60	35.030
✓ ISO/IEC 27556:2022 Information security, cybersecurity and privacy protection — User-centric privacy preferences management framework	60.60	35.030

4. Evolution of ISO 27000 (j)

✓ ISO/IEC 27557:2022	60.60	35.030
Information security, cybersecurity and privacy protection — Application of ISO 31000:2018 for organizational privacy risk management		
✓ ISO/IEC 27559:2022	60.60	35.030
Information security, cybersecurity and privacy protection – Privacy enhancing data de-identification framework		
✓ ISO/IEC TS 27560:2023	60.60	35.030
Privacy technologies — Consent record information structure		
✓ ISO/IEC TR 27563:2023	60.60	35.020
Security and privacy in artificial intelligence use cases — Best practices		
✓ ISO/IEC TS 27570:2021	60.60	35.030
Privacy protection — Privacy guidelines for smart cities		
✓ ISO/IEC 27701:2019	90.92	35.030
Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines		

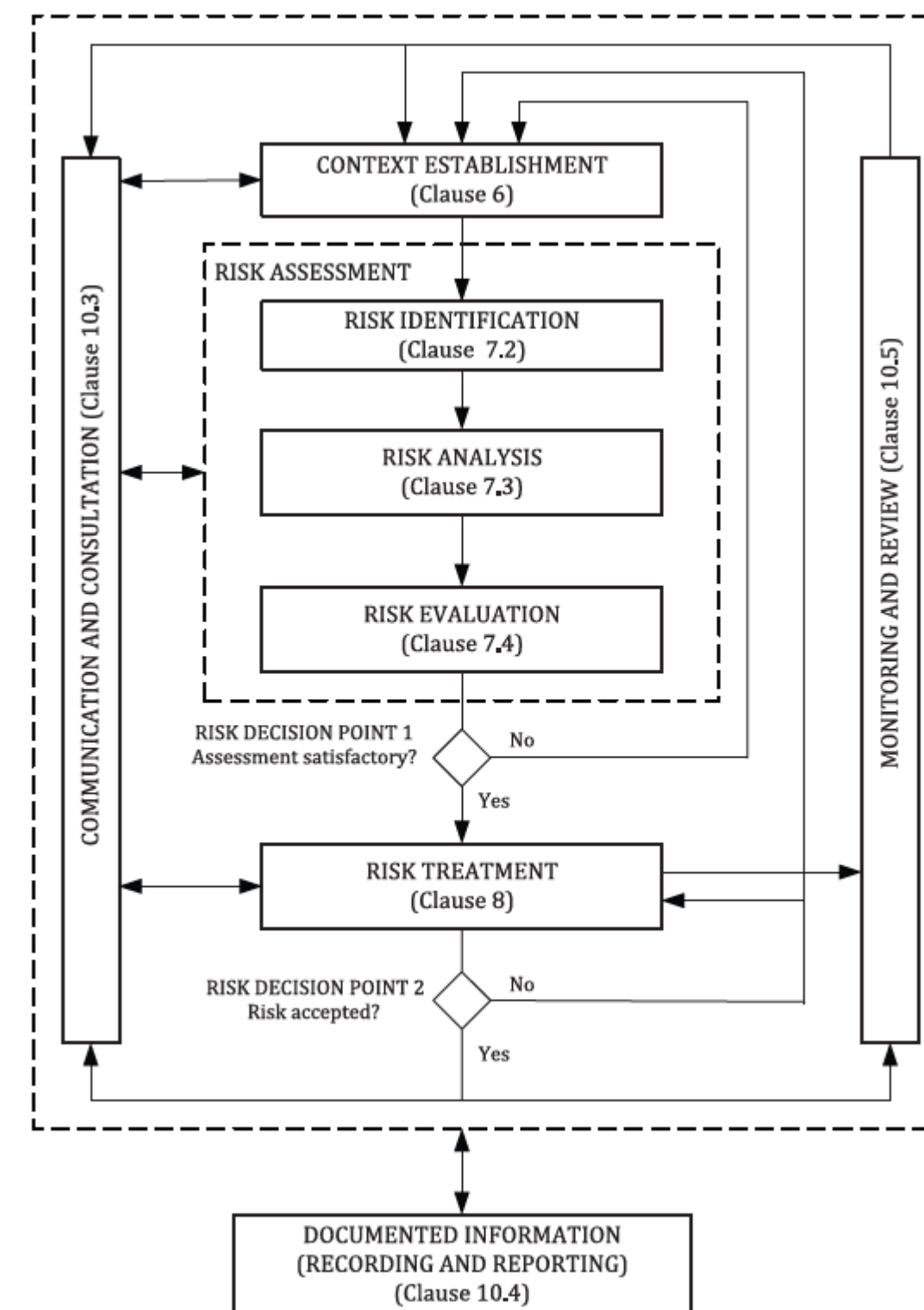
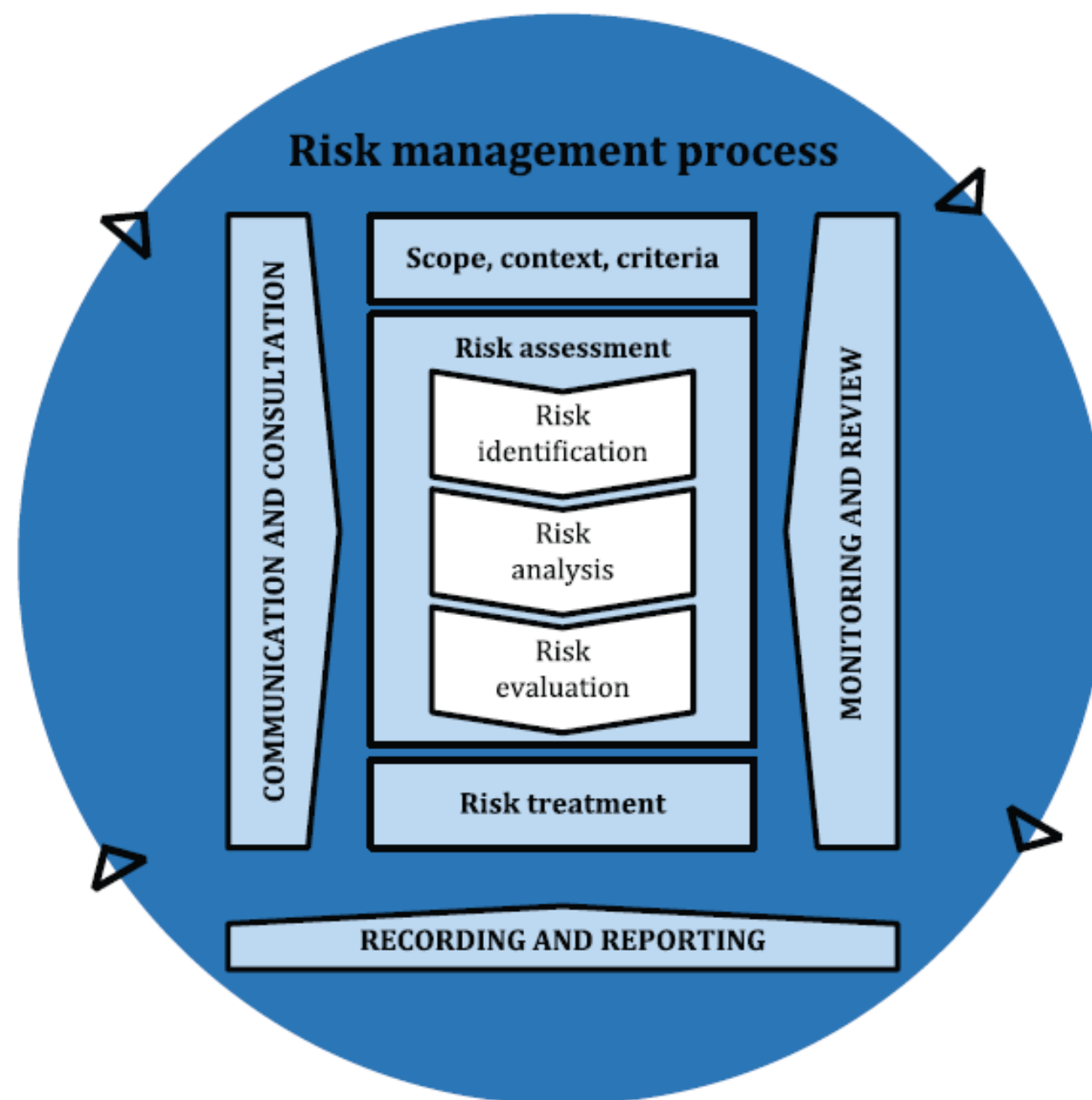
5. Evolution of ISO 27005



6. Risk Management by ISO 31000

Východisko pre všetky MSS normy – ako sú ISO 9000 a pod.

De facto **generický** štandard – ostatné štandardy špecificky aplikujú podľa priemyselnej oblasti, resp. domény



6. Risk Management by ISO 31000

6.4 Risk assessment

6.4.1 General

Risk assessment is the overall process of risk identification, risk analysis and risk evaluation.

6.4.2 Risk identification

- tangible and intangible sources of risk;
- causes and events,
- threats and opportunities;
- vulnerabilities and capabilities;
- changes in the external and internal context;
- indicators of emerging risks;
- the nature and value of assets and resources;
- consequences and their impact on objectives;
- limitations of knowledge and reliability of information;
- timeframes and time influences;
- biases, assumptions and beliefs of those involved.

6.4.3 Risk analysis

Risk analysis should consider factors such as:

- the likelihood of events and consequences;
- the nature and magnitude of consequences;
- complexity and connectivity;
- time-related factors and volatility;
- the pace of change
- the effectiveness of existing controls;
- sensitivity and confidence levels.

6.4.4 Risk evaluation

- do nothing further;
- consider risk treatment options;
- undertake further analysis to better understand the risk;
- maintain existing controls;
- reconsider objectives.

6. Risk Management by ISO 31000

6.5 Risk treatment

6.5.1 General

The purpose of risk treatment is to select and implement options for addressing risk.

Risk treatment involves an iterative process of:

- formulating and selecting risk treatment options;
- planning and implementing risk treatment;
- assessing the effectiveness of that treatment;
- deciding whether the residual risk is acceptable;
- if not acceptable, taking further treatment.

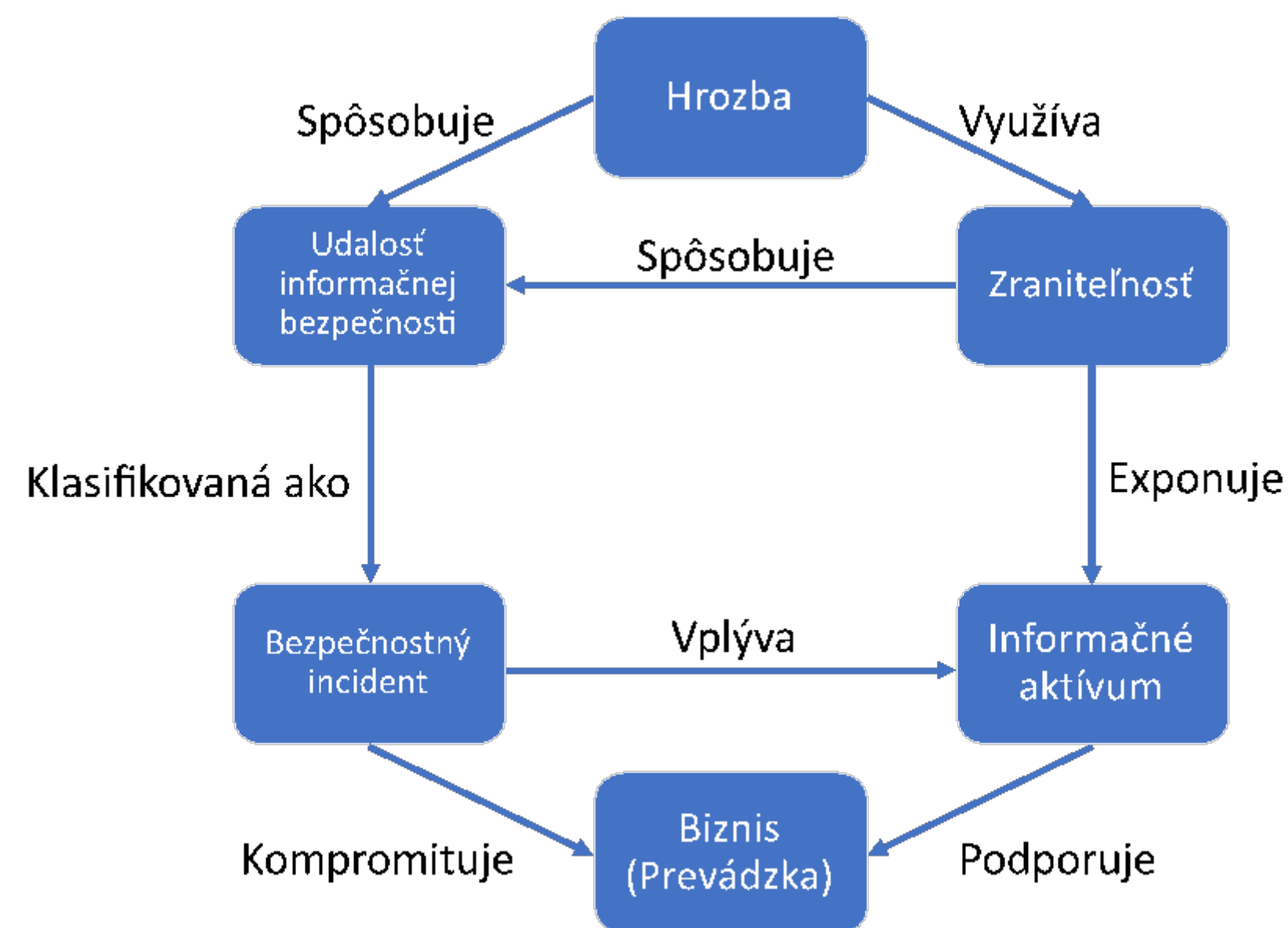
6.5.2 Selection of risk treatment options

- avoiding the risk by deciding not to start or continue with the activity
- taking or increasing the risk in order to pursue an opportunity;
- removing the risk source;
- changing the likelihood;
- changing the consequences;
- sharing the risk (e.g. through contracts, buying insurance);
- retaining the risk by informed decision.

6.5.3 Preparing and implementing risk treatment plans

- the rationale for selection of the treatment options, including the expected benefits to be gained;
- those who are accountable and responsible for approving and implementing the plan;
- the proposed actions;
- the resources required, including contingencies;
- the performance measures;
- the constraints;
- the required reporting and monitoring;
- when actions are expected to be undertaken and completed;

7. Risk Management by ISO 27005



7. Risk Management by ISO 27005

Asset-Event-Threat-Vulnerability-Consequence

7 Information security risk assessment process

7.1 General

The organization should use the organizational risk assessment process (if established) to assess risks to information or to define an information security risk assessment process.

Risk assessment enables risk owners to prioritize risks aligned with the treatment perspective, based primarily on their consequences and likelihood or other established criteria.

The context of the risk assessment should be determined including a description of scope and purpose as well as internal and external issues that affect the risk assessment.

Risk assessment consists of the following activities:

- a) risk identification, which is a process to find, recognize and describe risks (further details on risk identification are provided in [7.2](#));
- b) risk analysis, which is a process to comprehend the types of risk and to determine the level of risk. Risk analysis involves consideration of the causes and sources of risk, the likelihood that a specific event occurs, the likelihood that this event has consequences and the severity of those consequences (further details on risk analysis are provided in [7.3](#));
- c) risk evaluation, which is a process to compare the results of risk analysis with risk criteria to determine whether the risk and/or its significance is acceptable and to prioritize the analysed risks for risk treatment. Based on this comparison, the need for treatment can be considered (further details on risk evaluation are provided in [7.4](#)).

7. Risk Management by ISO 27005

7.2 Identifying information security risks

7.2.1 Identifying and describing information security risks

The risks identified should be those that, if they materialize, can have an effect on the achievement of the objectives.

ISO/IEC 27001:—¹), 6.1.2 c), requires the organization to define and apply an information security risk assessment process that identifies the information security risks. There are two approaches commonly used to perform risk identification:

- a) **event-based approach:** identify strategic scenarios through a consideration of risk sources, and how they use or impact interested parties to reach those risk's desired objective;
- b) **asset-based approach:** identify operational scenarios, which are detailed in terms of assets, threats and vulnerabilities.

In an event-based approach, the underlying concept is that risks can be identified and assessed through an evaluation of events and consequences. Events and consequences can often be determined by a discovery of the concerns of top management, risk owners and the requirements identified in determining the context of the organization (ISO/IEC 27001:—¹), Clause 4).

7. Risk Management by ISO 27005

Asset-Event-Threat-Vulnerability-Consequence

With an **asset-based approach**, the underlying concept is that risks can be identified and assessed through an inspection of **assets, threats and vulnerabilities**. An asset is anything that has value to the organization and therefore requires protection. Assets should be identified, taking into account that an information system consists of activities, processes and information to be protected. The assets can be identified as the primary and the supporting assets according to their type and priority, highlighting their dependencies, as well as their interactions with their risk sources and the organization's interested parties. **A threat exploits a vulnerability of an asset** to compromise the confidentiality, integrity and/or availability of corresponding information. If all valid combinations of assets, threats and vulnerabilities can be enumerated within scope of the ISMS, then, in theory, all the risks would be identified. For further steps of risk assessment, a list of assets associated with information and information-processing facilities should be drawn up.

The asset-based approach can identify asset-specific threats and vulnerabilities and allows the organization to determine specific risk treatment on a detailed level.

7. Risk Management by ISO 27005

Asset-Event-Threat-Vulnerability-Consequence

A.2.2 Assets

When applying the asset-based approach to the risk identification, the assets should be identified.

In the risk assessment process, within the development of risk scenarios, the identification of events, consequences, threats, vulnerabilities, should be linked to assets.

In the risk treatment process, each control is applicable to a subset of the assets.

The assets can be divided into two categories:

- primary/business assets - information or processes of value for an organization;
- supporting assets - components of the information system on which one or several business assets are based.

The primary/business assets are often used in the event-based approach (identification of events and their consequences on business assets).

The supporting assets are often used in the asset-based approach (identification and analysis of vulnerabilities and threats on these assets) and in the risk treatment process (specification of the asset(s) to which each control should be applied).

Business and supporting assets are related, therefore risk sources identified for supporting assets can impact business assets.

7. Risk Management by ISO 27005

Risk Source

Risk Source (A7)

- State-related
- Organised Crime
- Terrorist
- Ideological Activist
- Specialized Outfits
- Amateur
- Avenger
- Pathological attacker

Motivation (A8)

- Conquer
- Acquire
- Prevent
- Maintain
- Defend
- Survive

Target Objective (A9)

- Spying
- Strategic Pre-positioning
- Influence
- Obstacle to Functioning
- Lucrative
- Challenge, fun

DES-Desired End State

7. Risk Management by ISO 27005

Risk Qualitative Analysis

Table A.1 — Example of consequence scale

Consequences	Description
5 – Catastrophic	Sector or regulatory consequences beyond the organization Substantially impacted sector ecosystem(s), with consequences that can be long lasting. And/or: difficulty for the State, and even an incapacity, to ensure a regulatory function or one of its missions of vital importance. And/or: critical consequences on the safety of persons and property (health crisis, major environmental pollution, destruction of essential infrastructures, etc.).
4 – Critical	Disastrous consequences for the organization Incapacity for the organization to ensure all or a portion of its activity, with possible serious consequences on the safety of persons and property. The organization will most likely not overcome the situation (its survival is threatened), the activity sectors or state sectors in which it operates will likely be affected slightly, without any long-lasting consequences.
3 – Serious	Substantial consequences for the organization High degradation in the performance of the activity, with possible significant consequences on the safety of persons and property. The organization will overcome the situation with serious difficulties (operation in a highly degraded mode), without any sector or state impact.
2 – Significant	Significant but limited consequences for the organization Degradation in the performance of the activity with no consequences on the safety of persons and property. The organization will overcome the situation despite a few difficulties (operation in degraded mode).
1 – Minor	Negligible consequences for the organization No consequences on operations or the performance of the activity or on the safety of persons and property. The organization will overcome the situation without too much difficulty (margins will be consumed).

7. Risk Management by ISO 27005

Risk Qualitative Analysis

Table A.2 — Example of likelihood scale

Likelihood	Description
5 - Almost certain	The risk source will most certainly reach its objective by using one of the considered methods of attack. The likelihood of the risk scenario is very high.
4 - Very likely	The risk source will probably reach its objective by using one of the considered methods of attack. The likelihood of the risk scenario is high.
3 - Likely	The risk source is able to reach its objective by using one of the considered methods of attack. The likelihood of the risk scenario is significant.
2 - Rather unlikely	The risk source has relatively little chance of reaching its objective by using one of the considered methods of attack. The likelihood of the risk scenario is low.
1 - Unlikely	The risk source has very little chance of reaching its objective by using one of the considered methods of attack. The likelihood of the risk scenario is very low.

7. Risk Management by ISO 27005

Risk Qualitative Analysis

Table A.3 — Example of qualitative approach to risk criteria

Likelihood	Consequence				
	Catastrophic	Critical	Serious	Significant	Minor
Almost certain	Very high	Very high	High	High	Medium
Very likely	Very high	High	High	Medium	Low
Likely	High	High	Medium	Low	Low
Rather unlikely	Medium	Medium	Low	Low	Very low
Unlikely	Low	Low	Low	Very low	Very low

Table A.6 — Example of evaluation scale combined with three-colour risk matrix

Level of risk	Risk evaluation	Description
Low (green)	Acceptable as is	The risk can be accepted without further action.
Moderate (amber)	Tolerable under control	A follow-up in terms of risk management should be conducted and actions should be set up in the framework of continuous improvement over the medium and long term.
High (red)	Unacceptable	Measures for reducing the risk should absolutely be taken in the short-term. Otherwise, all or a portion of the activity should be refused.

7. Risk Management by ISO 27005

Risk Quantitative Analysis

Table A.4 — Example logarithmic likelihood scale

Approximate average frequency	Log expression	Scale value
Every hour	(approximately 10^5)	5
Every 8 hours	(approximately 10^4)	4
Twice a week	(approximately 10^3)	3
Once a month	(approximately 10^3)	2
Once a year	(10^1)	1
Once a decade	(10^0)	0

Table A.5 — Example logarithmic consequence scale

Consequence (a loss of)	Log expression	Scale value
£1 000 000	(10^6)	6
£100 000	(10^5)	5
£10 000	(10^4)	4
£1 000	(10^3)	3
£100	(10^2)	2
Less than £100	(10^1)	1

7. Risk Management by ISO 27005

Asset-Event-Threat-Vulnerability-Consequence

Examples of typical Threats (A10)

- Physical Threats (6) – Fire, water, Explosion ...
- Natural Threats (6) – Clima, Seismic, Volcano ...
- Infrastructure Failures (8) – Supply, Cooling, Power ...
- Technical Failures (3) – Failure of Device ...
- Human Actions (26) – Sabotage, Social Engineering ...
- Compromise of Functions(4) – Error in Use ...
- Organisational Threats (4) – Lack of Resources ...

57

D – Deliberate
A – Accidental
E – Environmental

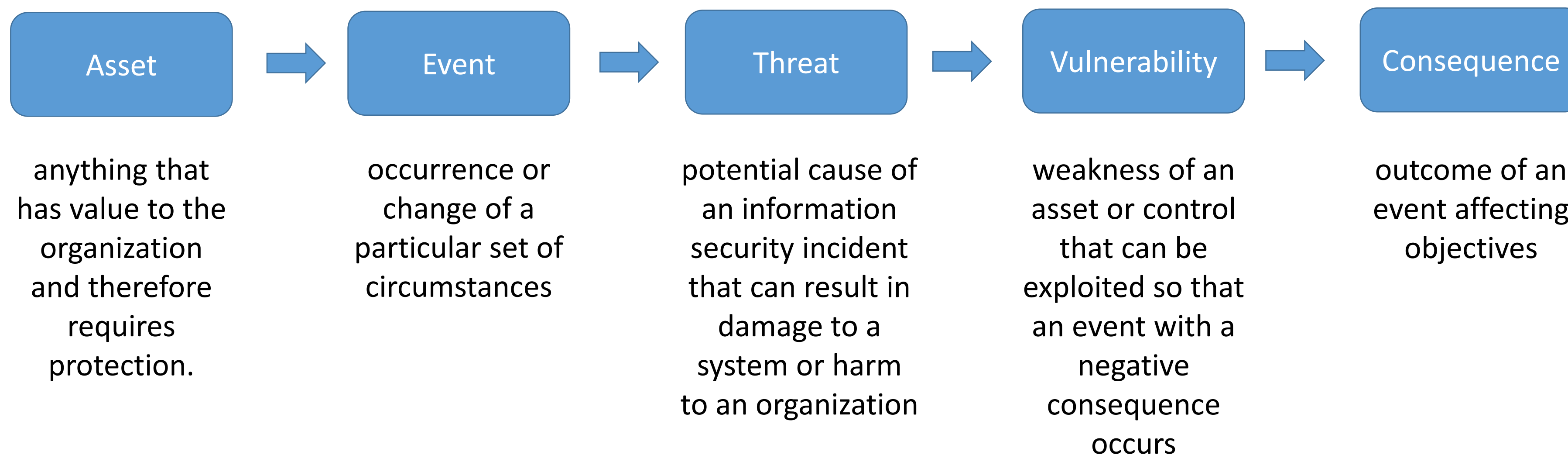
Examples of typical Vulnerabilities (A11)

- Hardware (10) – Un sufficient Maintenance of media ...
- Software (22) – Insufficient Software Testing ...
- Network (10) – Unprotected Lines ...
- Personnel (8) – Insufficient Training ...
- Site (4) – Inadequate physical access ...
- Organisation (28) – Missing procedures ...

82

7. Risk Management by ISO 27005

RISK = effect of uncertainty on objectives



8. Summary

ISO 31000:2018

- Pojmy threat (2 výskyty) a vulnerability (1 výskyt) nie sú definované
- Definované všetky relevantné procesy a artefakty
- Slúži ako generický model pre ostatné odvetvia
- Norma sa vôbec nevenuje praktickej implementácii protirizikových opatrení
- Normu si nemusíte kupovať – už je aplikovaná do ISO 27005

ISO/IEC 27005:2022

- Pojmy threat (52 výskytov) a vulnerability (12 výskytov) sú definované
- Norma je plne kompatibilná s ISO 31000
- Jedna jediná príloha A s 13 tabuľkami
- Norma obsahuje 5 ilustračných diagramov
- Všetky tabuľky v prílohe sú len odporúčané príklady
- Všetky tabuľky v prílohe sú Ready-To-Use
- Príloha A2.2 sa venuje informačným aktívam ale v obmedzenom rozsahu oproti predchádzajúcej verzii
- Norma nedáva jednoznačný alebo komplexný návod na vyhodnocovanie informačných rizík v línii asset-threat-vulnerability
- Pripravuje sa preklad do SK (bilingválna verzia)
- Normu si určite kúpte a primerane aplikujte (187 CHF)



Contact Us



rkormanak@gmail.com



+421 915 711 745



<https://www.linkedin.com/in/robert-kormanak-268b153/>



Ďakujem za pozornosť
