ISO 27 and NIS/NIS2

Koenraad Béroudiaux

- Lead Auditor ISO 27001 for BSI
- Accreditation auditor ISO 17021/27006 for Belac
- Expert in ISO/IEC JTC 1/SC 27/WG 1
- IRCA Principal auditor 6065184
- DPO qualified
- On ISO 27001 since 2013

*ISO27001-equivalence mentioned in the NIS1-law might have lead to **a misperception that governance aspects are considered more important** than technical measures, training and awareness campaigns*

This International Standard specifies the requirements for establishing, implementing, maintaining and continually improving an information security **management system** within the context of the organization.

This International Standard also includes requirements for the assessment and treatment of information security risks tailored to the needs of **the organization** (and beyond?).

The requirements set out in this International Standard are generic and are intended to be applicable to all organizations, regardless of type, size or nature.

Excluding any of the requirements specified in Clauses 4 to 10 is not acceptable when an organization claims conformity to this International Standard.

ISO/IE 27001 next ed. Beyond Information security

Resolution 2022/76 – Title change of ISO/IEC 27001

SC 27 resolves to change the title of ISO/IEC 27001 from:

“Information technology — Security techniques — Information security management systems — Requirements”

to

“Information security, cybersecurity and privacy protection — Information security management system – Requirements”

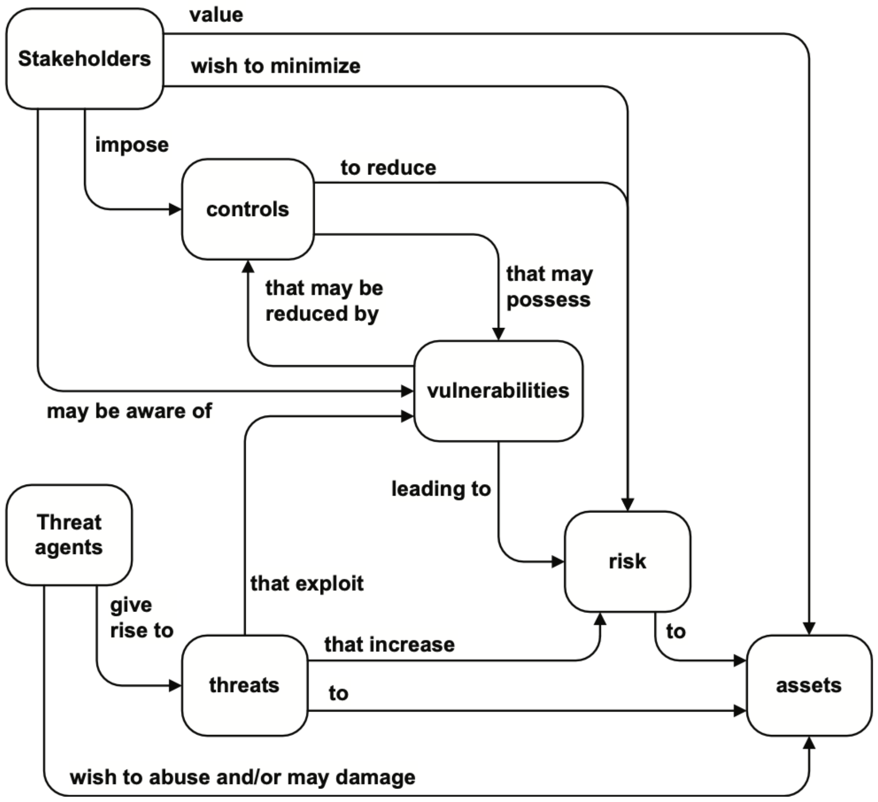
ISO/IEC TS 27100 (1st ed. 2020-10-13) Cybersecurity - Overview and Concepts

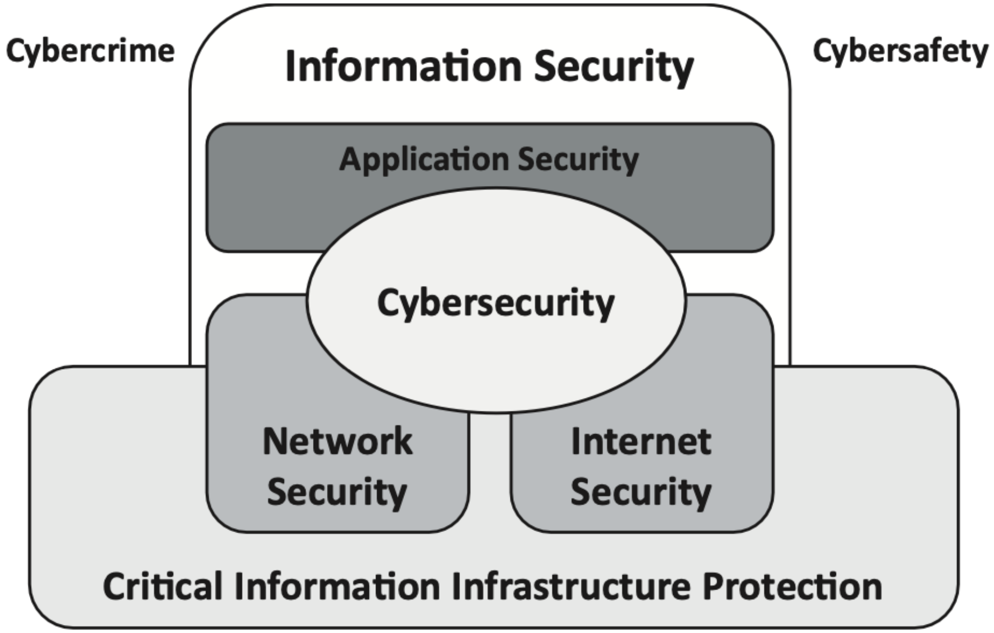
The objective of adequate cybersecurity is to maintain an acceptable level of **stability, continuity, and safety** of entities operating in cyberspace. While it is not possible to always achieve these objectives, cybersecurity aims to reduce cyber risks to a tolerable level.

Areas of concern for cybersecurity include:
a) stability and continuity of **society, organizations and nations**;
b) **property** (including information) of people and organizations; and
c) human **lives and health**.

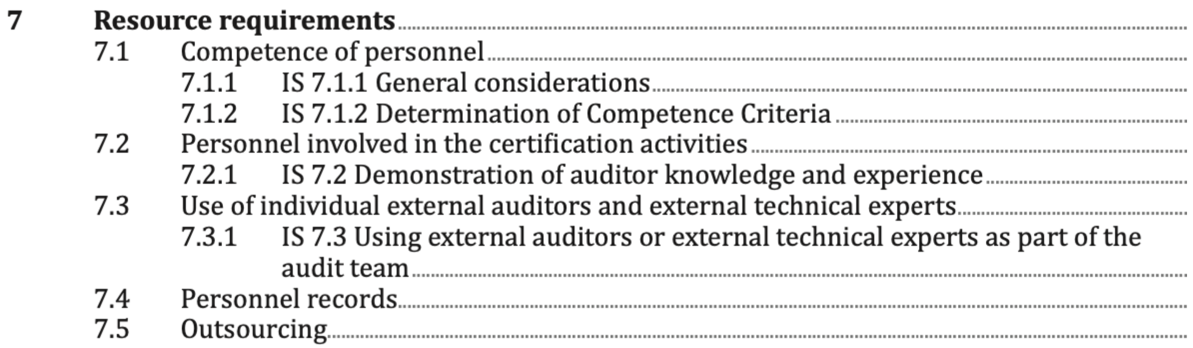
Cybersecurity with these characteristics is implemented by individual organizations. In cyberspace, organizations need to consider not only themselves, but also other parties who share cyberspace. While an organization needs to manage its vulnerabilities to ensure that the organization does not adversely affect other actors, it needs to work with others to reduce cyber risks. In addition, cybersecurity needs to reduce social and human losses in real space caused by cybersecurity incidents in cyberspace. Therefore, immediate detection and appropriate response of information security incidents are important elements of cybersecurity.

ISO/IEC 27032: 2012 *Information technology — Security techniques — Guidelines for cybersecurity*





ISO/IEC 27006:2015 Information technology — Security techniques — Requirements for bodies providing audit and certification of information security management systems



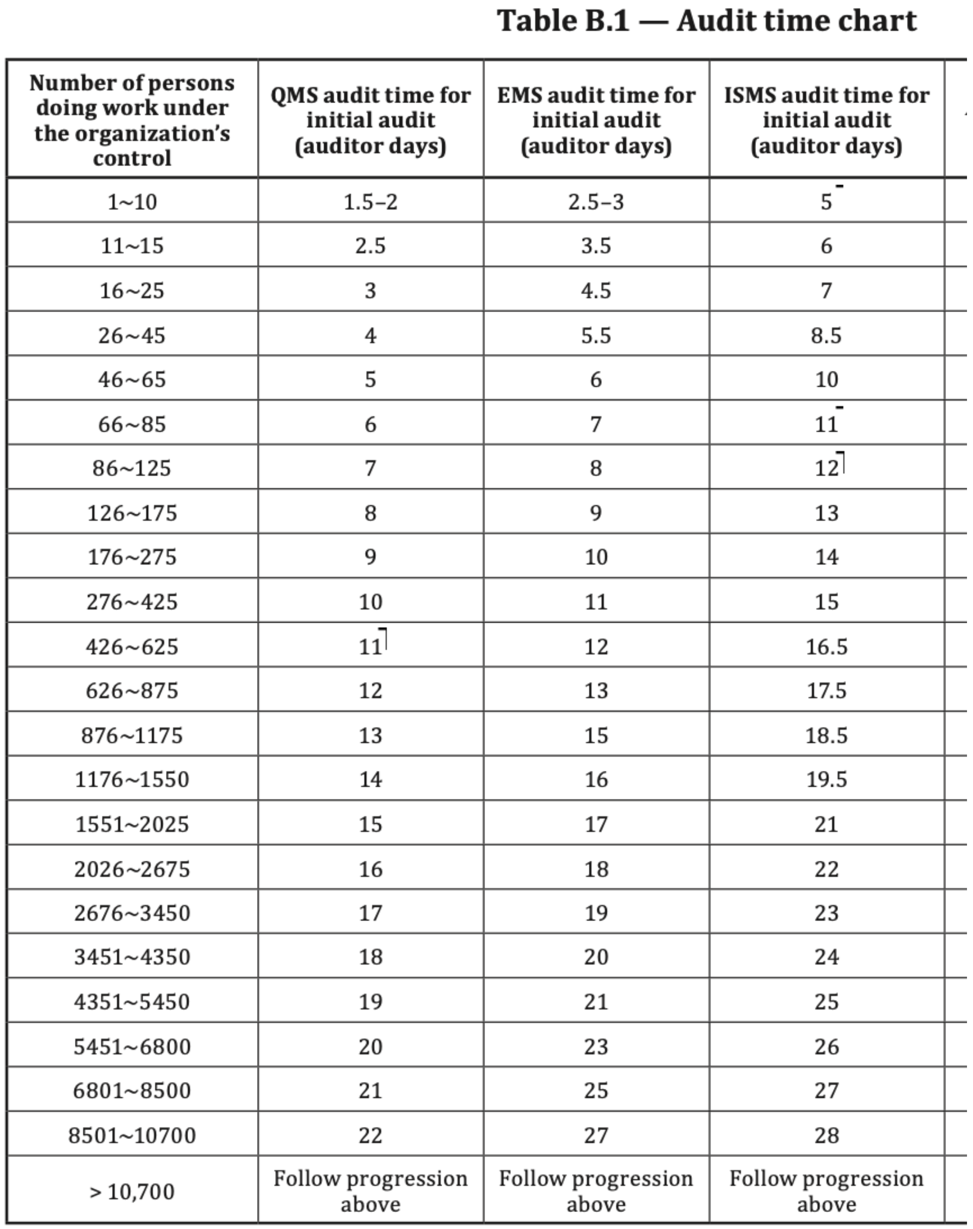


Table B.1 — Audit time chart

Number of persons doing work under the organization's control	QMS audit time for initial audit (auditor days)	EMS audit time for initial audit (auditor days)	ISMS audit time for initial audit (auditor days)
1~10	1.5–2	2.5–3	5
11~15	2.5	3.5	6
16~25	3	4.5	7
26~45	4	5.5	8.5
46~65	5	6	10
66~85	6	7	11
86~125	7	8	12
126~175	8	9	13
176~275	9	10	14
276~425	10	11	15
426~625	11	12	16.5
626~875	12	13	17.5
876~1175	13	15	18.5
1176~1550	14	16	19.5
1551~2025	15	17	21
2026~2675	16	18	22
2676~3450	17	19	23
3451~4350	18	20	24
4351~5450	19	21	25
5451~6800	20	23	26
6801~8500	21	25	27
8501~10700	22	27	28
> 10,700	Follow progression above	Follow progression above	Follow progression above

ISO IEC 27001:2013 Risks and opportunities §6.1.1 General (or inherent risks)

Management or Governance

Can the ISMS achieve its intended outcome?

What about undesired effects?

Any blocking factors for continual improvement?

§4: Poor understanding of internal or external issues; needs and expectations of interested parties; interfaces and dependencies between activities (internal the organisation or those performed by other organisations)

§5: Weak leadership commitment, shallow policies, ineffective organisations **(ownership!)**

§6.1: Incomplete risk assessment and risk treatment processes

§6.2: Vague objectives

§7.1-3: Insufficient resources, competences or awareness

§7.4-5: Poor communication and documentation

§8.1: Ineffective planning and control

§9: High level performance evaluation

§10: Little improvement

ISO IEC 27001:2013 §6.1.2 & §8.2 Information Security Risk Assessment

identify the **risk owners**

risk **acceptance** criteria *

criteria for performing information security risk assessments

consistent, valid and comparable results

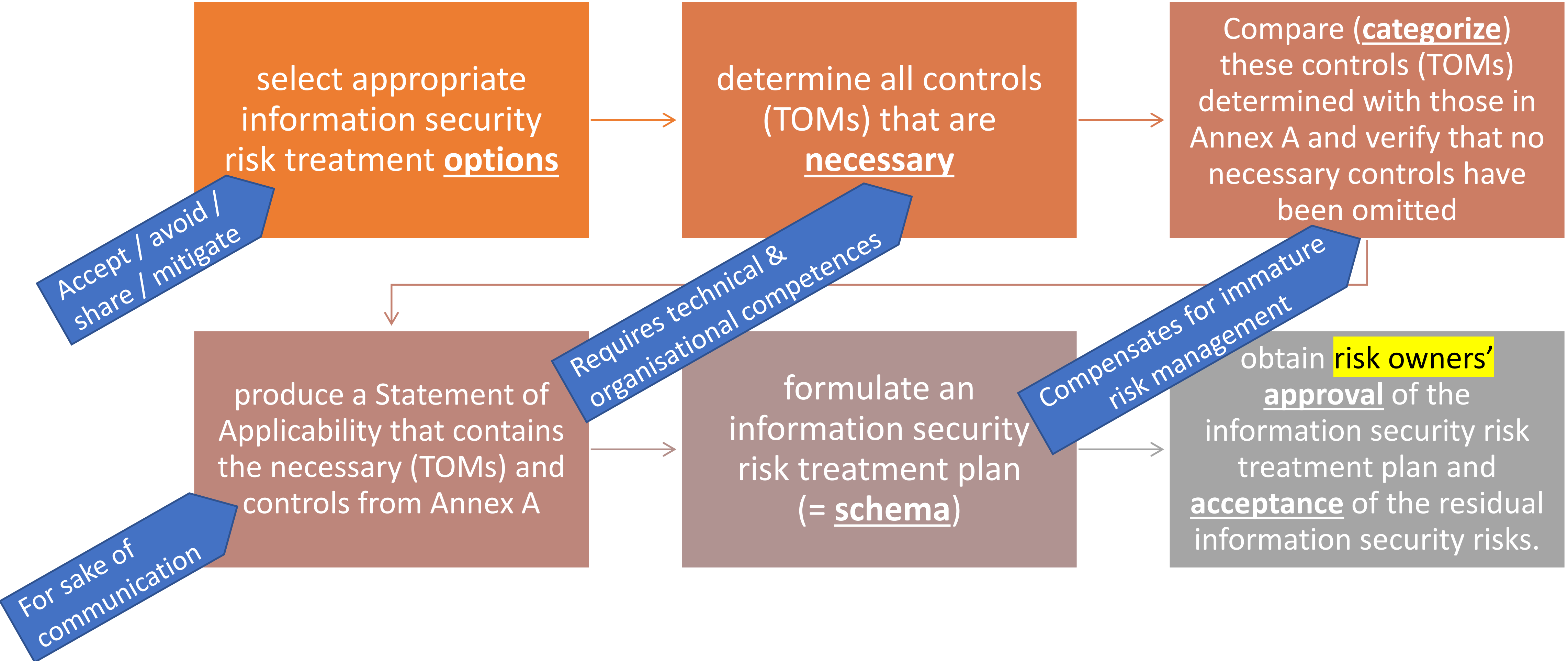
risks associated with the **loss of confidentiality, integrity and availability** for **information within the scope** of the ISMS (not: causes, threats or weaknesses, but may be part of the process to estimate likelihood)

- the potential **consequences** (incl. cyber & personal) *
- the realistic **likelihood** (between very very small and very small)

compare the results of risk analysis with the risk criteria *

prioritize the analysed risks for treatment

ISO IEC 27001:2013 §6.1.3 & §8.3
Information Security Risk Treatment



select appropriate information security risk treatment **options**

Accept / avoid / share / mitigate

determine all controls (TOMs) that are **necessary**

Requires technical & organisational competences

Compare (**categorize**) these controls (TOMs) determined with those in Annex A and verify that no necessary controls have been omitted

Compensates for immature risk management

produce a Statement of Applicability that contains the necessary (TOMs) and controls from Annex A

For sake of communication

formulate an information security risk treatment plan (= **schema**)

obtain risk owners' **approval** of the information security risk treatment plan and **acceptance** of the residual information security risks.

Annex A, a.k.a.
ISO/IEC 27002:2022
Information security, cybersecurity and privacy protection — Information security controls

§2: There are no normative references in this document.

§4.1 Structure of controls

a) 37 Organizational
b) 8 People
c) 14 Physical
d) 34 Technological

Only a guidance:
Still too abstract
Not auditable

No definition of ‘good’, but ‘Purpose’ is good food for thought

§4.3: Control layout

Control title: Short name of the control;

Attribute table: A table shows the value(s) of each attribute for the given control;

Control: What the control is;

Purpose: Why the control should be implemented;

Guidance: How the control should be implemented;

Other information: Explanatory text or references to other related documents.

27001§8.1 Operational planning and control

The organization shall plan, implement and control the **processes** needed to meet information security requirements, and to implement the actions determined in §6.1. The organization shall also implement plans to **achieve** information security **objectives** determined in §6.2.

What does *'Good'* look like?

It's all very recursive

§4.2: the needs and expectations (**requirements)** of interested parties relevant to information security

§5.1.e&f: **ensuring** that the information security management system achieves its **outcome**(s); and directing and supporting persons to contribute to the **effectiveness** of the ISMS

§5.3.b: **reporting** on the performance of the ISMS

§6.1.2.c.2: identify the **risk owners**

§6.1.3.f: obtain risk owners' **approval** of the information security risk treatment plan and acceptance of the residual information security risks

§6.2.b&j: be **measurable**; how the results will be **evaluated**

§7.1-3: **determine and provide the resources** needed; determine the **necessary competence**s; **contribution** to the effectiveness; and **implications** of not conforming

§7.4-5: determine the **need** for internal and external communications; documentation is **available and suitable for use**

§8.1: the organization shall keep documented information to the extent necessary to have **confidence** that the processes have been carried out as planned

§9.1: Monitoring, measurement, analysis and **evaluation**

§9.2.d: define the **audit criteria**

§9.3: Top management shall review the organization's information security management system at planned intervals **to ensure its continuing suitability, adequacy and effectiveness**.

§10.1.d: review the **effectiveness** of any corrective action taken

What is the difference between a TOM and a control?

ISO/IEC 27000:2016 2.16 **control:** measure that **is** modifying *risk*

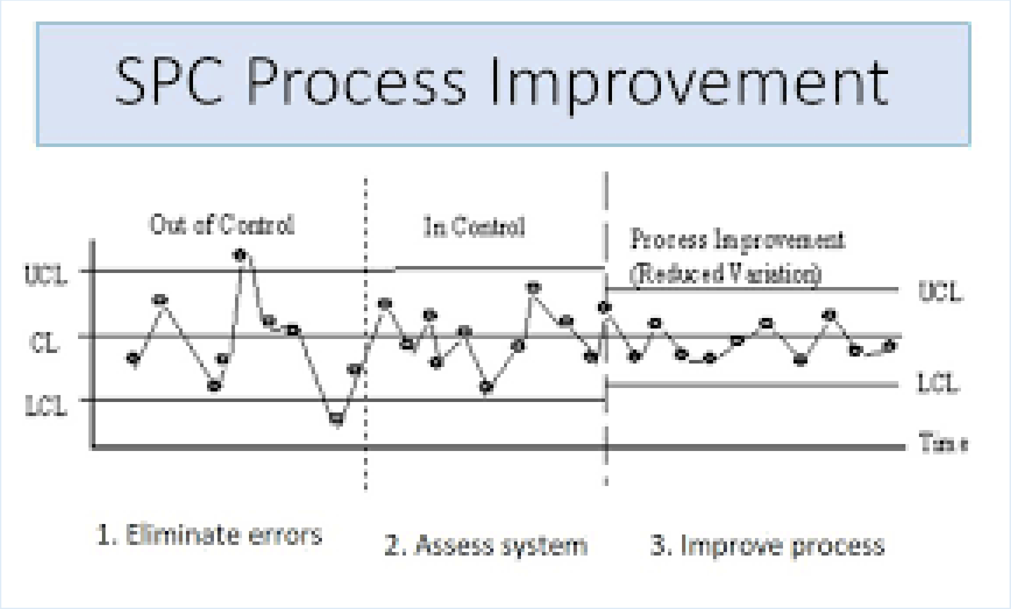
‘Is’ as in “no doubt”, ”no assumptions”, within “control limits” (SPC), to the level of “accepted risk”.

To ensure: to make sure that something happens or is definite

To assure: to make yourself certain about something

ISO 27002: a whole lot of measures

ISO 27001: ensure that risks are effectively modified to assure interested parties



To be “in control” is a concept of statistical process control.

ISO 27001 and NIS/NIS2: possible major nonconformities for ISO27001 certification

Are the **requirements** clear?

How to **report** on performance? (Reporting on incidents is not very assuring).

Who is the **risk owner**? Who **approves** the risk treatment schemas?

Are the objectives measurable, are there any evaluation **criteria**?

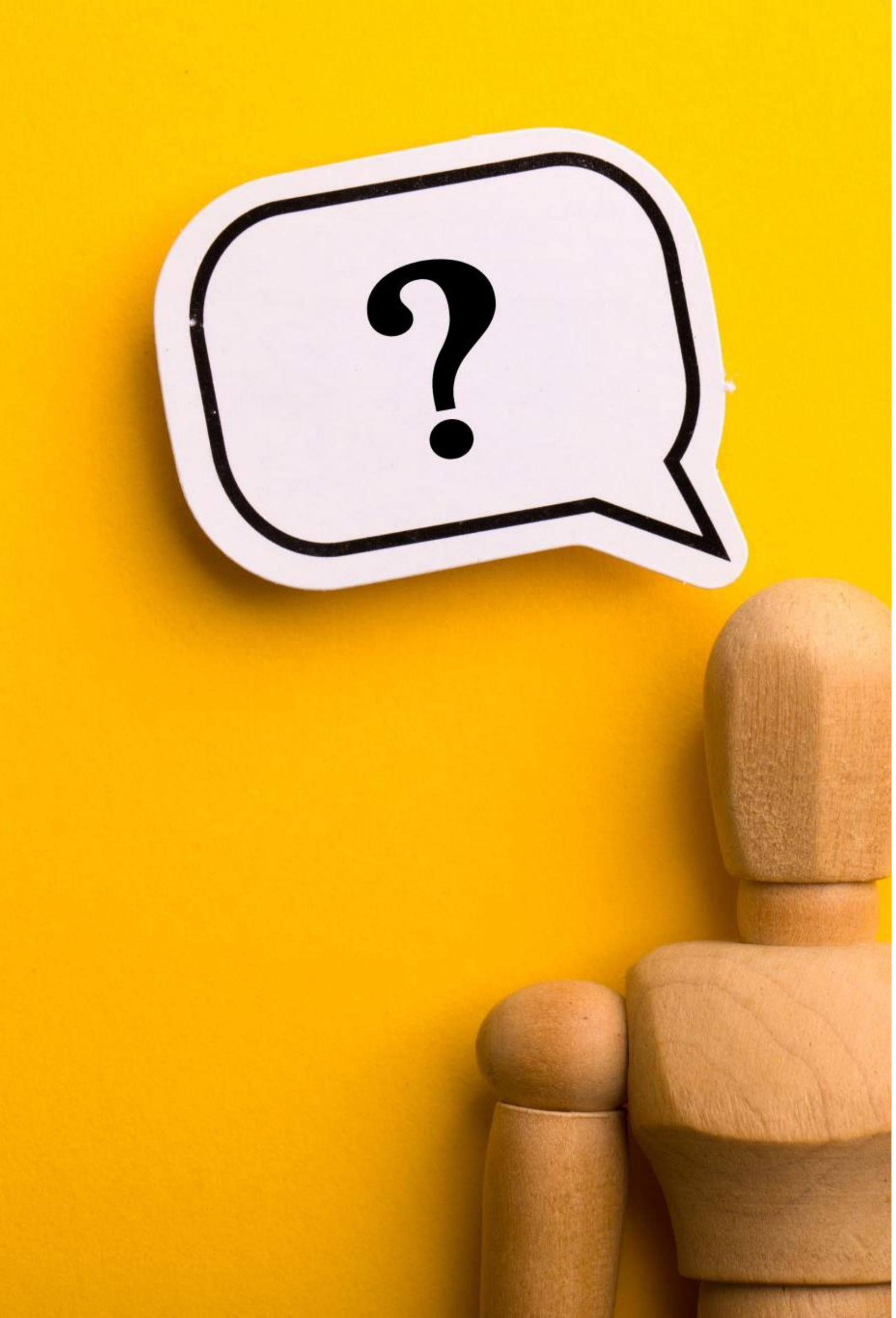
Are there specific requirements for qualifications/**competences**?

What **monitoring data** is required for evaluation?

What specific **audit criteria** have been defined?

On what grounds can top management **decide** about suitability, adequacy and effectiveness?

I don’t want to go to jail



Questions and discussion

□
😎
😱
👽