WEBINAR RECORDED

PECB

Navigating the Transition: From ISO/IEC 27701:2019 to ISO/IEC 27701:2025

NOVEMBER 26 | 03:00 PM CET

Peter Geelen

Cybersecurity Expert and Managing Director of CyberMinute

Connect at LinkedIN

https://www.linkedin.com/in/pgeelen/

#GlobalLeadingVoices

PECB CERTIFIED TITANIUM TRAINER

MVP Microsoft® Most Valuable Professional

Agenda

- Back in time
- PIMS vs ISMS
- Back to the future
- ISO 27701: 2025 Highlights
- Mastering the transition
- What about audit?
- Useful references
- Q&A

PECB

Back in time

ISO 27701 - PIMS

PIMS <> ISMS

- ISO 27001
  - Information Security
  - ISMS
- ISO 27701
  - Privacy Information
  - PIMS
- Audit (Certification)
  - ISO 27006
  - ISO 27706

Where we come from… where we go to

The ISMS/PIMS Timeline

- ISO27001:2013
  - Cor1:2014
  - Cor2:2015
  - + national standards (local translation)
- ISO/IEC 27006:2015
  - ISO/IEC 27006:2015/Amd 1:2020
- ISO27701:2019
- ISO/IEC TS 27006-2:2021
- ISO27001:2022
- ISO/IEC 27001:2022/Amd 1:2024
- ISO/IEC 27006-1:2024
- ISO27701:2025
- ISO/IEC 27706:2025

Where we come from… where we go to

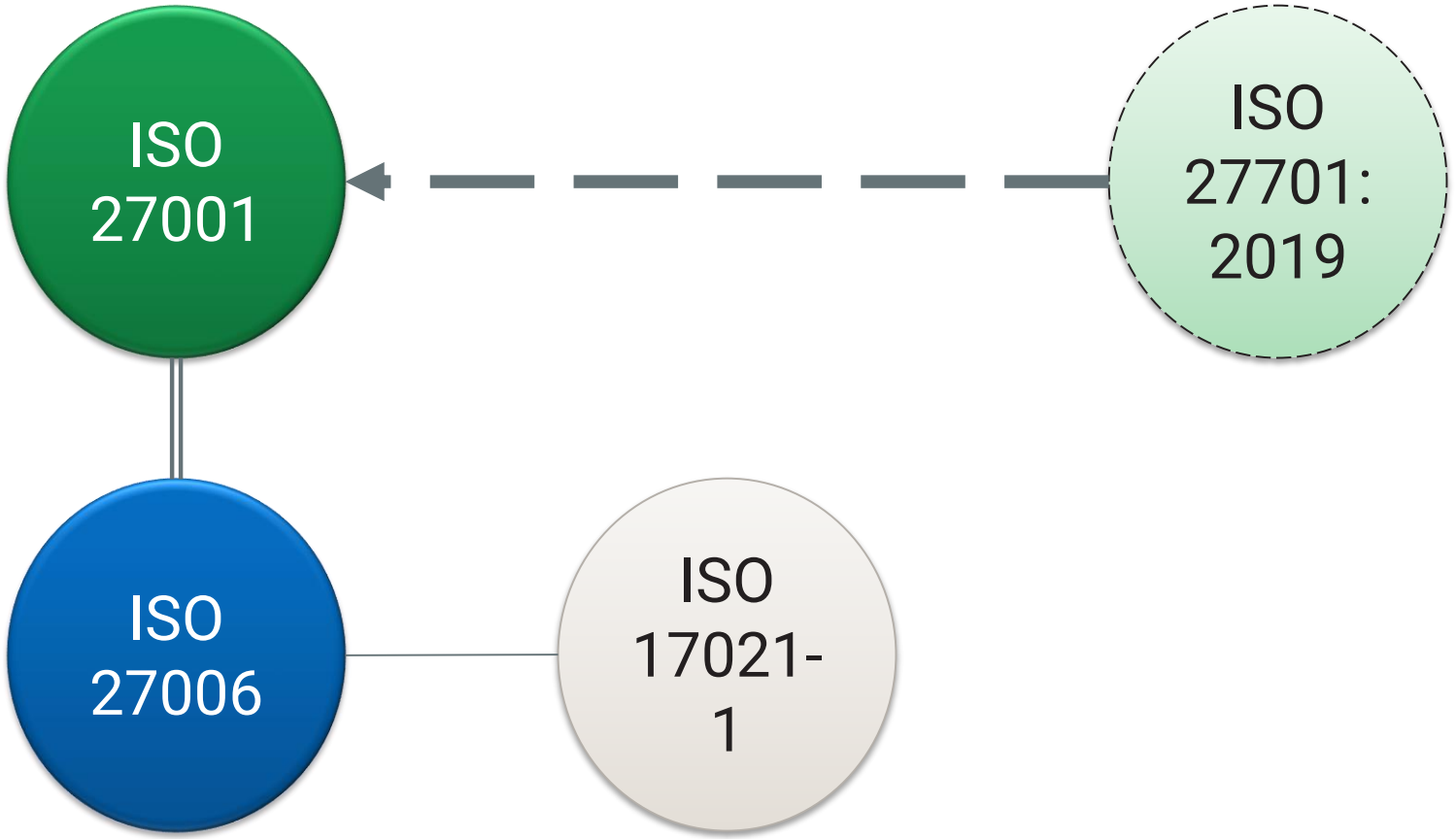
The ISMS/PIMS Timeline

- ISO27001:2013
  - Cor1:2014
  - Cor2:2015
  - + national standards (local translation)
- ISO/IEC 27006:2015
  - ISO/IEC 27006:2015/Amd 1:2020
- ISO27701:2019
- ISO/IEC TS 27006-2:2021
- ISO27001:2022
- ISO/IEC 27001:2022/Amd 1:2024
- ISO/IEC 27006-1:2024
- ISO27701:2025
- ISO/IEC 27706:2025

PIMS vs ISMS

Where we come from… where we go to

The ISMS/PIMS relation was



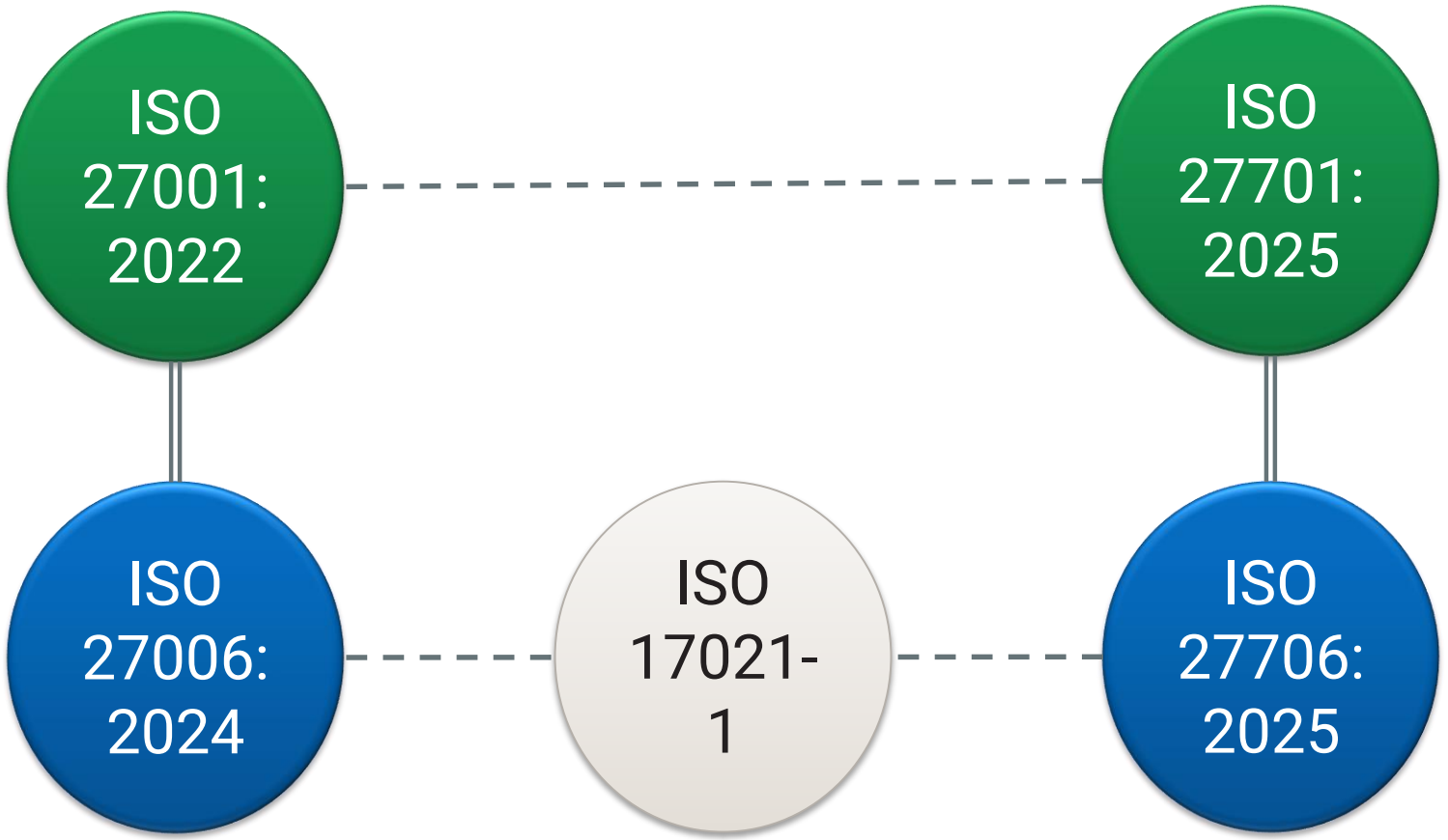
Where we come from… where we go to

The ISMS/PIMS link

- ISO 27701:2019
  - Extension of ISO 27001
  - Integrated approach with ISO 27001
- ISO 27001 structure
  - 10 Clauses (PDCA = C5>10)
  - Annex A (2022: 93 controls)
- ISO 27701:2019
  - 8 clauses
    - C5: PIMS > ISMS
    - C6: PIMS > ISO 27002
    - C7: Guidance for Controllers
    - C8: Guidance for processors
  - 7 annexes (A>F)

Where we come from… where we go to

The ISMS/PIMS relation now



PECB

Where we come from… where we go to

The ISMS/PIMS link

- ISO 27701:2025
  - Standalone
  - Structure aligned with HLS (indirectly with ISO 27001)
- ISO 27001:2022 structure
  - 10 Clauses (PDCA = C5>10)
  - Annex A (93 controls)
- ISO 27701:2025
  - 10+1 clauses
  - 7 annexes (A>F)
    - A (normative): PIMS reference control for controllers+processors
    - B (Normative): Implementation guidance
    - C (informative): mapping to ISO29100 privacy framework
    - D (informative): mapping to GDPR
    - E (informative): mapping to 27018+29151
    - F (informative) mapping 27701:2019 > 27701:2025

Structure of ISO/IEC 27701:2019 vs 2025

Comparison

ISO/IEC 27701:2019	ISO/IEC 27701:2025
Foreword	*Foreword*
Introduction	*Introduction*
1 Scope	*1 Scope*
2 Normative references	*2 Normative references*
3 Terms, definitions and abbreviations	*3 Terms, definitions and abbreviations*
4 General	*4 Context of the organization*
5 PIMS-specific requirements related to ISO/IEC 27701	*5 Leadership*
6 PIMS-specific guidance related to ISO/IEC 27001	*6 Planning*
7 Additional ISO/IEC 27002 guidance for PII controllers	*7 Support*
8 Additional ISO/IEC 27002 guidance for PII processors	*8 Operation*
	9 Performance evaluation
	10 Improvement
	11 Further information on annexes

Structure of ISO/IEC 27701:2019 vs 2025

Comparison

ISO/IEC 27701:2019	ISO/IEC 27701:2025
Annex A (normative) PIMS-specific reference control objectives and controls (PII Controllers)	*Annex A (normative) PIMS reference control objectives and controls for PII controllers and PII processors*
Annex B (normative) PIMS-specific reference control objectives and controls (PII Processors).	*Annex B (normative) Implementation guidance for PII controllers and PII processors*
Annex C (informative) Mapping to ISO/IEC 29100	*Annex C (informative) Mapping to ISO/IEC 29100*
Annex D (informative) Mapping to the General Data Protection Regulation	*Annex D (informative) Mapping to the General Data Protection Regulation*
Annex E (informative) Mapping to ISO/IEC 27018 and ISO/IEC 29151	*Annex E (informative) Mapping to ISO/IEC 27018 and ISO/IEC 29151*
Annex F (informative) How to apply ISO/IEC 27701 to ISO/IEC 27001 and ISO/IEC 27002	*Annex F (informative) Correspondence with ISO/IEC 27701:2019*
Bibliography	*Bibliography*

Back to the future

ISO 27701:2025

What's new?

- ISO/IEC 27701, Normative references
  - 2019 edition, referenced
    - ISO/IEC 27000,
    - ISO/IEC 27001, and
    - ISO/IEC 27002,
    - reflecting its role as an extension of the ISO/IEC 27001 information security framework.
  - 2025 revision
    - removes these references and
    - retains only ISO/IEC 29100
    - marking a clear shift from dependency on the 27000 series to a privacy-focused foundation.

ISO 27701:2025

What's new?

- Terminology in ISO/IEC 27701:2025
  - Clause 3, *Terms, definitions and abbreviations,* in ISO/IEC 27701:2025 has been completely expanded and modernized compared with the 2019 version.
  - removes all dependency on ISO/IEC 27000, referencing only ISO/IEC 29100, and
  - introduces **25 standardized terms**
    - aligned with the harmonized structure (HS) used across ISO management system standards (e.g., "organization," "top management," "policy," "risk," "continual improvement," "audit," etc.).
  - PIMS = independent management system (not just an extension of ISMS)

ISO 27701:2025: Annexes

What's new?

Annex A (normative), *PIMS reference control objectives and controls for PII controllers and PII processors*

- retained content from 2019
  - but **restructured** for clarity and traceability
- Consolidates control objectives for both **PII controllers and processors**
- Aligns control numbering and wording with the 2025 clause structure
  - (no longer mapped directly to ISO/IEC 27001 or ISO/IEC 27002)
- **statement of applicability** (SoA) required
- clearer guidance for inclusion/exclusion of controls
- risk-treatment justification

ISO 27701:2025: Annexes

What’s new?

Annex B (normative), *Implementation guidance for PII controllers and PII processors*

- fully rewritten and **expanded implementation guidance** replacing the 2019 guidance that was split between clauses 7 and 8
- practical detail for applying Annex A controls
- Integrates privacy-risk concepts from **ISO/IEC 27557**, improving consistency in assessment and treatment

ISO 27701:2025: Annexes

What’s new?

Annex C (informative), *Mapping to ISO/IEC 29100*

- Consists of retained and **updated terminology** for the eleven privacy principles
- Clarifies how the 2025 PIMS requirements correspond to the ISO/IEC 29100:2024 framework
- Includes editorial alignment only; **no structural change** to the principle-mapping

ISO 27701:2025: Annexes

What’s new?

Annex D (informative), *Mapping to the General Data Protection Regulation*

- retained and **expanded cross-reference** between PIMS clauses and GDPR Articles 5-32
- clearer traceability for compliance demonstration and audit evidence

ISO 27701:2025: Annexes

What’s new?

Annex E (informative), *Mapping to ISO/IEC 27018 and ISO/IEC 29151*

- retained and **updated clause references** to reflect Annex A restructuring
- Ensures alignment of privacy and cloud-processing controls across standards

ISO 27701:2025: Annexes

What’s new?

Annex F (informative), *Correspondence with ISO/IEC 27701:2019*

- **transition matrix** between 2019 and 2025 editions
- Identifies controls that were **merged**, **renamed**, **or removed**
- official **crosswalk for migration and certification updates**

ISO 27701: 2025 Highlights

PECB

ISO 27701:2025

4. Context of organisation

- the scope expanded, when defining the PIMS context
  - requiring organizations to consider internal and external factors
  - such as legal, regulatory, and governance obligations, as well as climate change, when defining the PIMS context.
- clearer expectations to identify relevant interested parties and
- determine which of their requirements will be addressed.

ISO 27701:2025

PIMS

- Clause 4.4
  - replaces “information security management system” with “privacy information management system,”
  - signaling a shift toward a **holistic privacy governance** model rather than a security extension.

ISO 27701:2025

5. Leadership

Updates to the Structure of Clause 5

ISO/IEC 27701:2019	ISO/IEC 27701:2025
5.3 *Leadership*	5 *Leadership*
5.3.1 *Leadership and commitment*	5.1 *Leadership and commitment*
5.3.2 *Policy*	5.2 *Privacy policy*
5.3.3 *Organizational roles, responsibilities and authorities*	5.3 *Roles, responsibilities and authorities*

ISO 27701:2025

6. Planning

ISO/IEC 27701:2019	ISO/IEC 27701:2025
5.4 *Planning*	6 *Planning* (restructured and expanded)
5.4.1 *Actions to address risks and opportunities*	6.1 *Actions to address risks and opportunities*
5.4.1.1 *General*	6.1.1 *General*
5.4.1.2 *Information security risk assessment*	6.1.2 *Privacy risk assessment*
5.4.1.3 *Information security risk treatment*	6.1.3 *Privacy risk treatment*
5.4.2 *Information security objectives and planning to achieve them*	6.2 *Privacy objectives and planning to achieve them*
	6.3 *Planning of changes* (new clause)

ISO 27701:2025

6. Planning

- **ISO/IEC 27701:2025, clause 6.1.2**
  - The new clause defines a structured privacy risk assessment process with clear criteria for risk acceptance, consistency, and comparability.
  - It mandates identification of risk owners, analysis of likelihood and impact, evaluation against set criteria, and documentation of the entire process in line with ISO/IEC 27557.

ISO 27701:2025

6. Planning

- **6.3 Planning changes**
  - The 2025 edition introduces an additional clause within clause 6.
  - When the organization determines the need for changes to the privacy information management system, the changes shall be carried out in a planned manner.

ISO 27701:2025

7. Resources

ISO/IEC 27701:2019	ISO/IEC 27701:2025
5.5.1 *Resources*	7.1 *Resources*
5.5.2 *Competence*	7.2 *Competence*
5.5.3 *Awareness*	7.3 *Awareness*
5.5.4 *Communication*	7.4 *Communication*
5.5.5 *Documented information* 5.5.5.1 *General* 5.5.5.2 *Creating and updating* 5.5.5.3 *Control of documented information*	7.5 *Documented information* 7.5.1 *General* 7.5.2 *Creating and updating documented information* 7.5.3 *Control of documented information*

ISO 27701:2025

8. Operations

ISO/IEC 27701:2019	ISO/IEC 27701:2025
5.6 *Operation*	8 *Operation*
5.6.1 *Operational planning and control*	8.1 *Operational planning and control*
5.6.2 *Information security risk assessment*	8.2 *Privacy risk assessment*
5.6.3 *Information security risk treatment*	8.3 *Privacy risk treatment*

ISO 27701:2025

9. Performance evaluation

ISO/IEC 27701:2019	ISO/IEC 27701:2025
5.7 *Performance evaluation*	9 *Performance evaluation*
5.7.1 *Monitoring, measurement, analysis and evaluation*	9.1 *Monitoring, measurement, analysis and evaluation*
5.7.2 *Internal audit*	9.2 *Internal audit* 9.2.1 *General* 9.2.2 *Internal audit program*
5.7.3 *Management review*	9.3 *Management review* 9.3.1 *General* 9.3.2 *Management review inputs* 9.3.3 *Management review results*

ISO 27701:2025

10 Improvement

ISO/IEC 27701:2019	ISO/IEC 27701:2025
5.8 *Improvement*	10 *Improvement*
5.8.1 *Nonconformity and corrective action*	10.1 *Continual improvement*
5.8.2 *Continual improvement*	10.2 *Nonconformity and corrective action*

ISO 27701:2025

Annex A (normative)

- **structural transformation** rather than a rewrite.
- all privacy and information security controls into a **single annex**.
- contains
  - the PIMS reference control objectives and controls for **PII controllers and PII processors,**
  - which were previously distributed across Annex A and Annex B of ISO/IEC 27701:2019.
- The PIMS-specific guidance that was part of clause 6 in the 2019 version has now been **reorganized** and presented as Table A.3 within Annex A.

ISO 27701:2025

Annex B (normative)

- expands from a processor-only focus to include both **PII controllers and PII processors**.
- no longer lists control objectives;
  - instead, it provides **implementation guidance** for the PII controller and processor controls found in Annex A.
- implementation guidance previously in clauses 6, 7 and 8 of ISO/IEC 27701:2019 has now been moved to Annex B of ISO/IEC 27701:2025.
- harmonized new numbering aligned with Annex A tables (A.1-A.3)
  - improved consistency and traceability.
- orientation shifts from prescriptive control statements (“shall …”) to advisory guidance statements (“should …”).
- now fully self-contained, mapping to new Annex A (2025) instead of relying on ISO/IEC 27001:2013 Annex A.
- strategic realignment reflects ISO/IEC 27701’s transition into a **stand-alone PIMS** management system standard.

ISO 27701:2025

Annex C (informative)

- The naming of the tables in ISO/IEC 27701:2025 remains the same as in the ISO/IEC 27701:2019 version.
- The 2025 edition keeps the same structure and purpose for Annex C, adds cross-references to Tables A.1-A.3, and replaces “compliance” with “conformity” for consistency with ISO terminology.

ISO 27701:2025

Annex D (informative)

- The naming of the table in ISO/IEC 27701:2025 Annex D remains the same as in the 2019 version.
- The 2025 edition simplifies the wording, reformats the note, and clarifies that the mapping is indicative, with organizations responsible for assessing their legal obligations.

ISO 27701:2025

Annex E (informative)

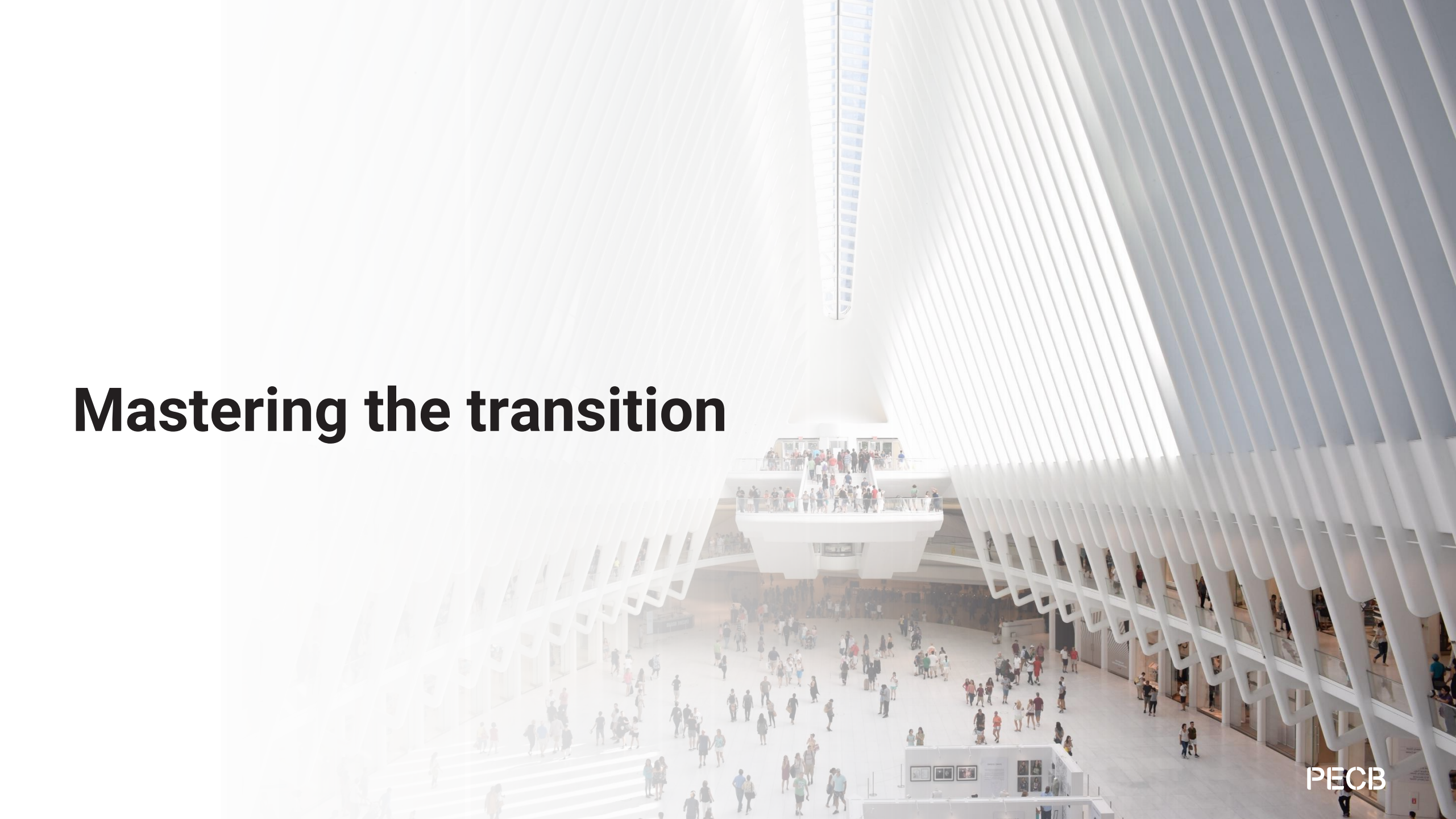
- The naming of the table in ISO/IEC 27701:2025 remains the same as in the 2019 version.
- The 2025 edition introduces a fully revised and expanded mapping table with updated clause references from ISO/IEC 27018 and ISO/IEC 29151.
- The introductory text has been simplified for clarity, emphasizing that the mapping is indicative and does not imply equivalence between provisions.

ISO 27701:2025

Annex F (informative)

- The naming and content of Annex F have been completely revised.
- The previous version, **“How to apply ISO/IEC 27701 to ISO/IEC 27001 and ISO/IEC 27002,”** has been replaced with **“Correspondence with ISO/IEC 27701:2019.”**
- The updated annex focuses on mapping and alignment with the previous edition rather than providing application guidance.

Mastering the transition



ISO 27701:2025

Main Steps to Master the Transition

- Learn how to support the PIMS of the organization by taking into account the requirements of ISO/IEC 27701:2025
- Identify the additional requirements and implement them
- Revise the documentation and the content of clauses 4 to 10 of ISO/IEC 27701:2025

PECB Course & certification transition

What is changing?

- The new ISO/IEC 27701:2025 has been published on 2025-10-14.
- PECB will be publishing
  - the ISO/IEC 27701:2025 Transition training course and exam,
  - alongside the updated training courses and certification exams for
    - Lead Auditor,
    - Lead Implementer,
    - Foundation.

PECB Course & certification transition

ISO/IEC 27701:2025 Transition course

Here are some important dates:

→ **2025-10-14 ISO has published the new ISO/IEC 27701:2025 standard**

→ **PECB will publish the ISO/IEC 27701 training scheme in English as follows:**

2025-11-07	ISO/IEC 27701:2025 Transition
2025-11-18	ISO/IEC 27701 Foundation
2025-11-18	ISO/IEC 27701 Lead Implemente
2025-12-18	ISO/IEC 27701 Lead Auditor

→ **In 2026, the courses will be available in other languages**

PECB

PECB Course & certification transition

Changes affect my current ISO/IEC 27701 certificate?

- The **new updates do not have an impact on your existing certification** against ISO/IEC 27701 standard.
- you just need to maintain these certifications
  - valid Implementer, Lead Implementer, Senior Lead Implementer or
  - Valid Auditor, Lead Auditor, or Senior Lead Auditor,
  - active by submitting CPDs and AMFs.
- However, PECB encourages certified individuals
  - to take the ISO/IEC 27701:2025 Transition course and exam,
  - to update their knowledge, and
  - report the course and exam as continuous professional development (CPDs) credits, as per the CPD Policy.
- For Foundation and ISO/IEC 27701 Provisional Implementer or Provisional Auditor, no maintenance is required.

PECB Course & certification transition

Effect on PECB Trainers

- trainers shall take the ISO/IEC 27701:2025 Transition course and exam to continue teaching the ISO 27701 courses
- The deadline to take the transition exam is October 14, 2026.

PECB Course & certification transition

More information

- https://pecb.com/pdf/iso-iec-27701-2025-transition-overview.pdf

What about audit?

What about the certification audits?

ISO 27701 vs ISO 27001

- ISO/IEC 27706-2025

Table A.1 — Audit time chart

Number of persons doing work under the organization's control involving the handling or processing of PII, or with access to such data		PII-controllers audit time for initial audit (auditor days)	PII-processors audit time for initial audit (auditor days)	PII-processor + controller audit time for initial audit (auditor days)	Additive and subtractive factors	Total audit time
1–10		4	3,5	6,5	See A.3.5	
11–15		4	3,5	6,5	See A.3.5	
16–25		5	4	6,5	See A.3.5	
26–45		5	4	7	See A.3.5	
46–65		6	4,5	8	See A.3.5	
66–85		6	4,5	9	See A.3.5	
86–125		7	5	10	See A.3.5	
126–175		7	5	11	See A.3.5	
176–275		8	5,5	12	See A.3.5	
276–425		8	6	12	See A.3.5	
426–625		9	6	14	See A.3.5	
626–875		10	7	15	See A.3.5	
876–1 175		11	7	16	See A.3.5	

ISO/IEC 27006-1:2024(en)

Table C.1 — Audit time chart

Number of persons doing work under the organization's control	Quality management system audit time for initial audit (auditor days, d)	Environmental management system audit time for initial audit (auditor days, d)	ISMS audit time for initial audit (auditor days, d)	Additive and subtractive factors	Total audit time
1–10	1,5–2	2,5–3	5	See C.3.5	
11–15	2,5	3,5	6	See C.3.5	
16–25	3	4,5	7	See C.3.5	
26–45	4	5,5	8,5	See C.3.5	
46–65	5	6	10	See C.3.5	
66–85	6	7	11	See C.3.5	
86–125	7	8	12	See C.3.5	
126–175	8	9	13	See C.3.5	
176–275	9	10	14	See C.3.5	
276–425	10	11	15	See C.3.5	
426–625	11	12	16,5	See C.3.5	
626–875	12	13	17,5	See C.3.5	

What about the certification audits?

- ISO/IEC 27706-2025
  - A.3.6: Limitation of deviation of audit time
    - Max 30%
- ISO 27001

Table D.4 — Impact of factors on audit time

		IT complexity		
		Low (from 3 to 4)	Medium (from 5 to 6)	High (from 7 to 9)
Business complexity	High (from 7 to 9)	+5 % to +20 %	+10 % to +50 %	+20 % to +100 %
	Medium (from 5 to 6)	−5 % to −10 %	0 %	+10 % to +50 %
	Low (from 3 to 4)	−10 % to −30 %	−5 % to −10 %	+5 % to +20 %

PECB

Useful references

Useful References

ISO/IEC 27701

- PECB Store > https://mypecb.com/store
  - Find 27701 : **ISO/IEC 27701:2025** (https://mypecb.com/store/view/497)

Useful References

ISO/IEC 27706

- PECB Store > https://mypecb.com/store
  - Find 27701 : **ISO/IEC 27701:2025** (https://mypecb.com/store/view/497)

Useful References

ISO standards

- ISMS: ISO 27001: https://www.iso.org/standard/27001
  - ISO/IEC 27001:2022/Amd 1:2024 (FREE): https://www.iso.org/standard/88435.html
- ISO/IEC 27006-1:2024: https://www.iso.org/standard/82908.html

- PIMS: ISO 27701: https://www.iso.org/standard/27701
- ISO/IEC 27706:2025: https://www.iso.org/standard/27706

- Internal audit
  - ISO 19011:2018: https://www.iso.org/standard/70017.html

- Accreditation
  - ISO/IEC 17021-1:2015: https://www.iso.org/standard/61651.html

Useful References

ISO standards

- ISO Information Security & Privacy Compliance Package
  - https://www.iso.org/publication/PUB200277.html
  - **ISO/IEC 27701:2025**
  - **ISO/IEC 27018:2025**
  - **ISO/IEC 27001:2022**

Useful References

Must Watch: IAF MD Documents (Mandatory documents)

- MD = mandatory documents for audit
  - https://iaf.nu/en/iaf-documents/?cat_id=7
  - IAF MD29:2024 Transition Requirements for ISO/IEC 27006-1:2024
  - IAF MD26:2023 Transition Requirements for ISO/IEC 27001:2022

Useful References

ISO vocabulary

- Normative vs informative (shall vs should)
- ISO Directives (Part 2)
  - https://www.iso.org/sites/directives/current/part2/index.xhtml
- Check chapter 7: Verbal forms for expressions of provisions
  - Chapter 7.2 Requirement (shall, shall not)
  - Chapter 7.3 Recommendation (should, should not)

- See also: https://identityunderground.wordpress.com/2024/06/03/training-notes-cimsa-interesting-reference-documents-for-iso-auditors/

Upskill your career with PECB Skills

15-minute courses on:

- AI
- Cybersecurity
- Data Protection
- Auditing
- Information Security

Earn CPDs for each competency and Get Certified

PECB Skills

THANK YOU

✉ peter@cyberminute.com
in https://www.linkedin.com/in/pgeelen/
✉ NIS Institute
in https://www.linkedin.com/company/nisinstitute/