ISO 27701 Control Checklist

Extending the ISMS for Privacy

A practical self-assessment checklist for a PIMS aligned with privacy governance, ISMS integration and operational evidence.

Working document for initial diagnosis, gap assessment and roadmap preparation.

What it includes

- 12 critical control domains
- 48 practical diagnostic questions
- Fields for status and evidence
- Useful for CISO, DPO, IT and compliance teams

How to use

- Review one theme at a time
- Mark Yes / Partial / No / N/A
- Record real evidence
- Prioritise gaps and owners

Assessment legend

Yes	Partial	No	N/A
Implemented and evidenced	Exists, but incomplete	Not implemented	Not applicable to scope

1. Context, Scope and Interested Parties

#	Control question	Status	Evidence / notes
1	Is the PIMS scope defined and aligned with the ISMS scope, including services, processes, systems, locations and relevant categories of personal data?	☐ Yes ☐ Partial ☐ No ☐ N/A	______________________________ _ ______________________________ _
2	Have internal and external interested parties, and their privacy-related requirements, been identified and reviewed periodically?	☐ Yes ☐ Partial ☐ No ☐ N/A	______________________________ _ ______________________________ _
3	Has the organisation documented the main data subjects, processing purposes and key personal data flows included in the PIMS?	☐ Yes ☐ Partial ☐ No ☐ N/A	______________________________ _ ______________________________ _
4	Are the interfaces between information security, privacy, legal, IT, HR, marketing and procurement formally clarified?	☐ Yes ☐ Partial ☐ No ☐ N/A	______________________________ _

#	Control question	Status	Evidence / notes
			______________________________ _

2. Leadership, Governance and Responsibilities

#	Control question	Status	Evidence / notes
1	Has top management approved privacy objectives, responsibilities, resources and reporting criteria for the PIMS?	☐ Yes ☐ Partial ☐ No ☐ N/A	______________________________ _ ______________________________ _
2	Are controller, joint controller, processor and subprocessor roles correctly identified and documented where applicable?	☐ Yes ☐ Partial ☐ No ☐ N/A	______________________________ _ ______________________________ _
3	Is there a RACI matrix or equivalent for privacy, including the CISO, DPO, IT, process owners and procurement?	☐ Yes ☐ Partial ☐ No ☐ N/A	______________________________ _ ______________________________ _
4	Are significant privacy decisions escalated, approved and recorded consistently?	☐ Yes ☐ Partial ☐ No ☐ N/A	______________________________ _ ______________________________ _

3. Processing Inventory and Data Mapping

#	Control question	Status	Evidence / notes
1	Does the organisation maintain an up-to-date record of processing activities, systems, data categories, recipients, retention periods and applicable bases?	☐ Yes ☐ Partial ☐ No ☐ N/A	______________________________ _ ______________________________ _
2	Can the organisation quickly locate where personal data is collected, stored, used, shared and deleted?	☐ Yes ☐ Partial ☐ No ☐ N/A	______________________________ _ ______________________________ _
3	Are data flows involving third parties, affiliates, cloud providers and SaaS tools identified and documented?	☐ Yes ☐ Partial ☐ No ☐ N/A	______________________________ _ ______________________________ _
4	Do significant system or process changes trigger a review of the inventory and related documentation?	☐ Yes ☐ Partial ☐ No ☐ N/A	______________________________ _ ______________________________ _

4. Lawfulness, Transparency and Purpose Limitation

#	Control question	Status	Evidence / notes
1	Does each processing activity have a defined purpose, clear operational logic and a properly documented basis?	☐Yes ☐Partial ☐No ☐N/A	_______________________________ _______________________________
2	Do privacy notices, policies and transparency texts reflect what actually happens in processes and systems?	☐Yes ☐Partial ☐No ☐N/A	_______________________________ _______________________________
3	Does data collection follow minimisation criteria and avoid unnecessary fields, attributes or retention?	☐Yes ☐Partial ☐No ☐N/A	_______________________________ _______________________________
4	Are purpose changes, new campaigns, new integrations or data re-use reviewed before going live?	☐Yes ☐Partial ☐No ☐N/A	_______________________________ _______________________________

5. Risk Assessment and Privacy by Design

#	Control question	Status	Evidence / notes
1	Are privacy risks affecting individuals assessed using clear, consistent and proportionate criteria?	☐Yes ☐Partial ☐No ☐N/A	_______________________________ _______________________________
2	Do new projects, applications, integrations or material changes include privacy by design and by default from the outset?	☐Yes ☐Partial ☐No ☐N/A	_______________________________ _______________________________
3	Are privacy requirements built into projects, change management, development and system acquisition?	☐Yes ☐Partial ☐No ☐N/A	_______________________________ _______________________________
4	Are decisions to accept, mitigate or treat privacy risks approved and recorded with supporting evidence?	☐Yes ☐Partial ☐No ☐N/A	_______________________________ _______________________________

6. Operational Controls and Protection of Personal Data

#	Control question	Status	Evidence / notes

#	Control question	Status	Evidence / notes
1	Do access controls over personal data follow need-to-know, segregation of duties and periodic review principles?	☐ Yes ☐ Partial ☐ No ☐ N/A	______________________________ _ ______________________________ _
2	Does the organisation protect personal data at rest, in transit, in backups and in test or support environments?	☐ Yes ☐ Partial ☐ No ☐ N/A	______________________________ _ ______________________________ _
3	Do logging, monitoring and incident management enable the detection of misuse, unauthorised access or relevant control failures?	☐ Yes ☐ Partial ☐ No ☐ N/A	______________________________ _ ______________________________ _
4	Are environments, privileged accounts and data exports appropriately controlled to reduce exposure risk?	☐ Yes ☐ Partial ☐ No ☐ N/A	______________________________ _ ______________________________ _

7. Third-Party and Processor Management

#	Control question	Status	Evidence / notes
1	Is due diligence performed for suppliers processing personal data, including technical, organisational and compliance-related criteria?	☐ Yes ☐ Partial ☐ No ☐ N/A	________________________________ _ ________________________________ _
2	Do processor contracts include documented instructions, confidentiality, sub-processing, incident handling and support for data subject rights?	☐ Yes ☐ Partial ☐ No ☐ N/A	________________________________ _ ________________________________ _
3	Does the organisation periodically review subprocessors, cloud services, external integrations and relevant risk changes?	☐ Yes ☐ Partial ☐ No ☐ N/A	________________________________ _ ________________________________ _
4	Is there evidence of oversight over critical suppliers, including assessments, meetings, action plans or follow-up?	☐ Yes ☐ Partial ☐ No ☐ N/A	________________________________ _ ________________________________ _

8. Retention, Deletion and Data Quality

#	Control question	Status	Evidence / notes
1	Are retention periods defined by data category, purpose, legal obligation and operational need?	☐ Yes ☐ Partial ☐ No ☐ N/A	________________________________ _ ________________________________ _
2	Are practical mechanisms in place for deletion, anonymisation or restriction when data is no longer needed?	☐ Yes ☐ Partial ☐ No ☐ N/A	________________________________ _ ________________________________ _
3	Does the organisation test or verify whether retention schedules are actually enforced in systems?	☐ Yes ☐ Partial ☐ No ☐ N/A	________________________________ _ ________________________________ _
4	Are there criteria for correction, update and quality of personal data relevant to the business and to individuals?	☐ Yes ☐ Partial ☐ No ☐ N/A	________________________________ _ ________________________________ _

9. Data Subject Rights

#	Control question	Status	Evidence / notes

#	Control question	Status	Evidence / notes
1	Is there a documented process for receiving, assessing, responding to and closing access, rectification, erasure and other applicable rights requests?	☐ Yes ☐ Partial ☐ No ☐ N/A	______________________________ _ ______________________________ _
2	Can the organisation locate personal data by system, process and third party within reasonable timeframes?	☐ Yes ☐ Partial ☐ No ☐ N/A	______________________________ _ ______________________________ _
3	Do teams understand when a request can be fulfilled, limited, refused or escalated for further assessment?	☐ Yes ☐ Partial ☐ No ☐ N/A	______________________________ _ ______________________________ _
4	Are requests and responses recorded with sufficient evidence to demonstrate consistency and control?	☐ Yes ☐ Partial ☐ No ☐ N/A	______________________________ _ ______________________________ _

10. Incident Management and Personal Data Breaches

#	Control question	Status	Evidence / notes
1	Does the incident response process clearly distinguish information security incidents from potential personal data breaches?	☐Yes ☐Partial ☐No ☐N/A	______________________________ _ ______________________________ _
2	Is there a structured assessment of impact on individuals, severity criteria and a documented notification decision process?	☐Yes ☐Partial ☐No ☐N/A	______________________________ _ ______________________________ _
3	Do security, privacy, legal and communications teams know when and how to collaborate in a relevant incident?	☐Yes ☐Partial ☐No ☐N/A	______________________________ _ ______________________________ _
4	Are incident records, root causes, corrective actions, lessons learned and follow-up maintained?	☐Yes ☐Partial ☐No ☐N/A	______________________________ _ ______________________________ _

11. Competence, Training and Awareness

#	Control question	Status	Evidence / notes
1	Do employees receive role-appropriate training on privacy, security and the handling of personal data?	☐Yes ☐Partial ☐No ☐N/A	______________________________ _ ______________________________ _
2	Do higher-exposure teams — HR, IT, marketing, support, sales and procurement — receive enhanced or specific training?	☐Yes ☐Partial ☐No ☐N/A	______________________________ _ ______________________________ _
3	Is there evidence of participation, effectiveness, periodic refresh and updates to training content?	☐Yes ☐Partial ☐No ☐N/A	______________________________ _ ______________________________ _
4	Are privacy topics embedded into onboarding, role changes and ongoing awareness campaigns?	☐Yes ☐Partial ☐No ☐N/A	______________________________ _ ______________________________ _

12. Monitoring, Audit and Continual Improvement

#	Control question	Status	Evidence / notes

#	Control question	Status	Evidence / notes
1	Has the organisation defined PIMS performance indicators such as rights handling, retention, incidents, third parties and corrective actions?	☐ Yes ☐ Partial ☐ No ☐ N/A	______________________________ _ ______________________________ _
2	Does the programme include internal audits, management reviews and formal follow-up of nonconformities and improvements?	☐ Yes ☐ Partial ☐ No ☐ N/A	______________________________ _ ______________________________ _
3	Is PIMS evidence organised and accessible for customers, internal audits, supplier assessments and due diligence?	☐ Yes ☐ Partial ☐ No ☐ N/A	______________________________ _ ______________________________ _
4	Is there a realistic continual improvement plan to strengthen integration across ISO 27701, ISO 27001 and applicable legal requirements?	☐ Yes ☐ Partial ☐ No ☐ N/A	______________________________ _ ______________________________ _

Suggested minimum evidence pack

Use this page to verify whether the PIMS can demonstrate control in a practical and auditable way.

Evidence	Available?
PIMS scope and interfaces with the ISMS	☐ Yes ☐ Partial ☐ No
Privacy, retention, third-party and incident management policies	☐ Yes ☐ Partial ☐ No
Records of processing activities and data mapping	☐ Yes ☐ Partial ☐ No
Role matrix: controller / processor / owners / DPO / CISO	☐ Yes ☐ Partial ☐ No
Privacy by design criteria and risk management records	☐ Yes ☐ Partial ☐ No
Processor and subprocessor contracts and assessments	☐ Yes ☐ Partial ☐ No
Logs of rights requests, incidents and corrective actions	☐ Yes ☐ Partial ☐ No
Metrics, internal audits and management review outputs	☐ Yes ☐ Partial ☐ No

Recommended next step: assign an owner per theme, collect evidence, prioritise gaps and define a phased implementation plan.

Need support to turn this checklist into a real programme? Talk to iCompliance.eu.