ISOIEC 27701:2019 Internal Audit Checklist Template

1. Context of the Organization (ISO/IEC 27701:2019 Clause 5.2)

Audit Item	Yes/No	Evidence/Remarks
Has the organization identified its role as a **PII controller** or **PII processor**?		
Are external and internal privacy-related issues that affect the organization's ability to achieve intended privacy outcomes documented?		
Has the organization identified relevant interested parties and their requirements with respect to the protection of PII?		
Are boundaries of the PIMS clearly defined, including interactions with third-party processors/controllers?		

2. Leadership (ISO/IEC 27701:2019 Clause 5.3)

Audit Item	Yes/No	Evidence/Remarks
Has top management demonstrated leadership and commitment to the protection of PII and the PIMS?		
Are roles, responsibilities, and authorities related to privacy management clearly assigned and documented?		
Is there a published privacy policy that is aligned with legal requirements and organizational goals for PII protection?		
Are privacy objectives established and communicated throughout the organization?		

3. Risk Assessment and Planning (ISO/IEC 27701:2019 Clause 5.4 & 5.5)

Audit Item	Yes/No	Evidence/Remarks

Has the organization conducted a privacy risk assessment, identifying privacy risks specific to the processing of PII?		
Are risks and opportunities related to the processing of PII properly considered and documented?		
Does the organization have documented plans for addressing privacy risks, including risk mitigation measures?		
Are privacy objectives integrated into the organization's broader risk management framework?		

4. Support (ISO/IEC 27701:2019 Clause 5.6 & 5.7)

Audit Item	**Yes/No**	**Evidence/Remarks**
Are adequate resources assigned for the implementation, maintenance, and improvement of the PIMS?		
Are personnel involved in the PIMS adequately trained on privacy requirements and the protection of PII?		
Is there documentation that ensures the proper management of PII, including data inventories, privacy notices, and data subject consent records?		
Are procedures in place to ensure that communication related to PII processing and protection is handled properly (both internal and external)?		

5. Operational Controls (ISO/IEC 27701:2019 Clause 6.2)

Audit Item	**Yes/No**	**Evidence/Remarks**
Are procedures for obtaining and managing data subject consent well-established and followed?		
Are mechanisms in place to respond to data subject requests, such as access, rectification, and erasure?		

Is PII collected and processed for specified, legitimate purposes?		
Are agreements in place with third-party processors that ensure PII protection in line with ISO/IEC 27701:2019?		
Are PII transfers (internally and externally) compliant with applicable legal and regulatory requirements?		
Are retention and disposal schedules for PII established and followed?		

6. Privacy by Design and Default (ISO/IEC 27701:2019 Clause 6.3)

Audit Item	Yes/No	Evidence/Remarks
Does the organization apply **privacy by design** principles when developing or updating products and services involving PII?		
Is the processing of PII limited to the minimum necessary to achieve specified purposes?		
Are default settings configured to provide the highest level of privacy protection?		

7. Monitoring and Evaluation (ISO/IEC 27701:2019 Clause 6.4 & 6.5)

Audit Item	Yes/No	Evidence/Remarks
Are regular internal audits of the PIMS conducted, covering all privacy-related processes and controls?		
Are nonconformities related to PII protection identified, documented, and addressed promptly?		
Are performance indicators in place for evaluating the effectiveness of the PIMS?		
Are privacy-related incidents (e.g., data breaches) monitored, reported, and reviewed?		

Are management reviews conducted to ensure the PIMS remains aligned with legal and organizational privacy requirements?		

8. Improvement (ISO/IEC 27701:2019 Clause 6.6)

Audit Item	Yes/No	Evidence/Remarks
Is there a formal process for continually improving the PIMS, taking into account changes in privacy laws and best practices?		
Are corrective actions for PII-related nonconformities effectively implemented and verified for compliance?		
Does the organization actively seek opportunities for improving its privacy practices?		

PII Controller-Specific Requirements (ISO/IEC 27701:2019 Clause 7)

Audit Item	Yes/No	Evidence/Remarks
Is there a process to identify and document all PII processed by the organization?		
Are privacy notices provided to data subjects that clearly explain how their PII will be processed?		
Are data subject rights (e.g., access, rectification, erasure) managed in accordance with applicable laws?		
Are data processing agreements in place with third parties, and do they include privacy clauses?		
Is there a process for notifying data subjects and regulators in the event of a data breach?		

PII Processor-Specific Requirements (ISO/IEC 27701:2019 Clause 8)

Audit Item	Yes/No	Evidence/Remarks

Are processing activities conducted only under the instruction of the PII controller?		
Are records of all processing activities maintained in compliance with legal requirements?		
Are appropriate technical and organizational measures in place to protect PII, including data encryption, access control, and incident response?		
Are subcontractors involved in the processing of PII approved by the PII controller, and are they subject to appropriate contractual obligations?		

This **Internal Audit Checklist** is specifically aligned with the **ISO/IEC 27701:2019** requirements for PII controllers and PII processors. It helps ensure a comprehensive audit of privacy practices and the effectiveness of the Privacy Information Management System (PIMS) in protecting personally identifiable information.