



ISO/IEC 27701:2019 Risk Assessment Template

1. General Information

- **Assessment Date:**
 - **Assessor Name:**
 - **Department/Process:**
 - **Reviewed By:**
 - **Next Review Date:**
-

2. PII Processing Activity Information

- **Activity Name/Description:**
 - **Purpose of Processing:**
 - **PII Controller/Processor:**
 - **Categories of PII Collected (e.g., names, addresses, health data):**
 - **Data Subjects Affected (e.g., employees, customers):**
 - **Legal Basis for Processing (e.g., consent, legitimate interest):**
-



3. Privacy Risk Identification

#	Risk Description	Potential Impact on Data Subject	Likelihood (Low, Medium, High)	Impact (Low, Medium, High)
1	Unauthorized access to PII	Violation of privacy, identity theft	High	High
2	Data breach during transfer	PII exposure to unauthorized parties	Medium	High
3	Failure to obtain consent	Non-compliance with data protection laws	Low	Medium

4. Existing Controls/Measures

For each identified risk, list the existing controls/measures in place to reduce the likelihood or impact of the risk.

#	Existing Controls	Effectiveness (Low, Medium, High)
1	Encryption of PII during transfer	High
2	Access control and multi-factor authentication	Medium
3	Automated consent management system	Medium

5. Risk Mitigation/Action Plan

For risks that require additional mitigation, list the actions that need to be taken to reduce privacy risks.



#	Action Plan	Responsible Person	Deadline
1	Implement role-based access controls	IT Manager	30/09/2024
2	Conduct privacy awareness training for staff	HR Manager	15/10/2024

6. Residual Risk Assessment

Once mitigation actions are taken, reassess the remaining risk.

Residual Risk (Low, Medium, High)

1 Low

2 Low

3 Medium

7. Conclusion and Recommendations

- Summary of overall risk exposure based on the identified risks and mitigation measures.
 - Any further recommendations to improve privacy risk management.
-

8. Sign-Off

- **Assessor Name:**



- **Signature:**
- **Date:**

This template helps guide the risk assessment process in ISO/IEC 27701:2019 compliance by ensuring a structured approach to privacy risk management and identifying actions to mitigate potential risks.