Privacy Assessment Report

# Privacy Assessment Report Overview

After identifying the risks in the privacy assessment phase, the PIA then moves on to the report phase. This phase is where the organization must decide what they will do to address the privacy risks identified in the privacy assessment phase. The report team should consider the following while assessing individual risks:

* Whether the risks are necessary or avoidable.
* How the risks could affect the goals of a system/process, or broader organizational goals.
* How changes could achieve a more appropriate balance between the system/process goals, the interests of affected patrons and the interests of the organization and third parties.
* Whether to bring in additional people or develop a plan for further consultation on particular risks.
* Whether the risks are significant enough that the system/process should not be implemented.

The report team should consider the following while assessing risk responses:

* Privacy by Design — consider how the organization can adopt privacy policies, procedures, and practices throughout all levels, departments, projects, services, etc.
* Data minimization — limiting the collection, storage, disclosure, and processing of patron data to the business needs of the system/process.
* Transparency — risk responses should be transparent to both the patron and the organization through privacy policies and notices.
* Accountability – a process to assess the effectiveness of each risk response should be set up and the report shared with stakeholders, including staff, patrons, and third parties.
* Training – consider how staff and patron privacy training can support privacy goals and mitigate risks.
* Impact — take into account the diversity of patrons affected by the system/process, and whether they may respond or be affected differently to the sharing of their personal information
* Privacy enhancing technologies — consider whether any privacy enhancing technologies can be used and the impact of privacy invasive technologies on operations and patrons.

# Risk Assessment Table - definitions

Risk ID and Risk Description – the ID assign to each risk and the brief description of the risk.

Likelihood – the chances that this risk will be realized. Categories:

* **Likely** – High chance that the risk will be realized. High risks are going to occur from time to time, for example equipment failure in a situation where no redundancy is in place.
* **Possible** – Medium chance that the risk will be realized. Not 100% guaranteed to happen, but can happen if certain common conditions are met.
* **Unlikely** – Risk unlikely to happen.

Severity – the level of impact if the risk is realized. Categories:

* **Severe –** There is significant, real damage to the library and/or to patrons. This impact fundamentally changes the lives and overall operations of the people and organizations involved on multiple levels.
* **Moderate** – There is harm to the library and/or to some patrons if the risk is realized. Damage is limited in scope and does not fundamentally affect lives and overall operations of people/organizations.
* **Minor** – There is a procedural issue that does not lead to significant damage.

Risk Response – the strategy to respond to the individual risk. Categories:

* **Accept** – Risk to organization or patron is low, or there are resource restrictions that prevent addressing the risk in other ways.
* **Transfer** – Risk can be better managed by another entity, product, or process.
* **Mitigate** – Limit risk through implementing privacy controls in the process or product.
* **Eliminate** – Make changes to product or process to avoid identified risk.

# Report Structure

Many PIAs are structured to give a brief overview of the PIA process, leading into the risk assessment recommendations. The **Risk Assessment Table** and **Risk Response Template** in this document can be used to report on risk assessment, though the templates can be modified to meet the specific needs of the organization.

This report is also important in detailing what has to happen next in addressing the risks found in the PIA process. This could include naming a new project team and project charge.

A sample outline of a Privacy Assessment Impact report is below. The outline can be adjusted based on the report audience’s needs and expectations.

1. Project introduction and background
   1. Brief description of system/process (or changes to system/process)
   2. Factors that led to PIA (Threshold Analysis summary)
   3. PIA project team and members
2. PIA
   1. Data Analysis
      1. Process: how information was collected, who was involved, when, etc.
      2. Results, including areas of concern or of particular relevancy to privacy
   2. Privacy Risk Assessment
      1. Summary of risks (Risk Assessment Table)
      2. Risk response details
3. Further Action
   1. Project management items: team, timeline, milestones
   2. Plans to reassess product or process once report’s recommendations on addressing risk are made

# Sources and Additional Resources

Briney, Kristin, Becky Yoose, John Mark Ockerbloom, and Shea Swauger. 2020. “A Practical Guide to Performing a Library User Data Risk Assessment in Library-Built Systems.” DLF Privacy and Ethics in Technology Working Group. <https://doi.org/10.17605/OSF.IO/V2C3M>.

Newfoundland and Labrador Centre for Health Information. 2013. *Full PIA Report Template.* Version 2.2.

Office of the Australian Information Commissioner. 2020. “Guide to Undertaking Privacy Impact Assessments.” <https://www.oaic.gov.au/privacy/guidance-and-advice/guide-to-undertaking-privacy-impact-assessments/>.

Questionmark Computing Limited. 2017. “Data Protection Impact Assessment.” (Template). <https://iapp.org/media/pdf/resource_center/questionmark-dpia-template_12-nov-2017%20%282%29.pdf>

Whitener, Michael L. 2012. “Conducting a Privacy Audit.” *The Corporate Counselor.* 27(3). <https://iapp.org/media/pdf/knowledge_center/Conducting_a_Privacy_Audit_-_The_Corporate_Counselor_-_July_2012.pdf>

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Risk ID | Risk Description | Likelihood | Severity | Risk Response |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

# Risk Assessment Table

# Risk Response Template

Copy the following template for each individual risk listed in the Risk Assessment Table

**Risk ID**:

**Risk Description**:

**Risk Response**:  Accept Transfer Mitigate Eliminate

**Risk Response Decision Rationale** (why was this response chosen? Of particular importance if decision to accept the risk is chosen.)

**Risk Response Strategy**

*Include the following:*

* What – what must happen to address the risk based on the decision above
* How – how the strategy will be implemented
* Who – which people will be involved in the response strategy, including the person(s) ultimately responsible for the response strategy?
* When – timing of the response strategy