State of Indiana Standard: Privacy Impact Assessment Methodology: *A NIST-Based Framework to Support Enhanced Privacy Protections within Government*

Version: 1.1 (5/25/2023)

TABLE OF CONTENTS

DEFINITIONS

Terms	Definitions
Data Processing	Any operation or set of operations which is performed on personal information or on sets of personal information, whether by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction.
Personal Information System	According to Indiana Code 4-1-6-1(a), a personal information system is "any recordkeeping process, whether automated or manual, containing personal information and the name, personal number, or other identifying particulars of a data subject."
Personal Information (PI)	According to Indiana Code 4-1-6-1(b), PI is any "information that describes, locates, or indexes anything about an individual or that affords a basis for inferring personal characteristics about an individual including, but not limited to, the individual's education, financial transactions, medical history, criminal or employment records, finger and voice prints, photographs, or the individual's presence, registration, or membership in an organization or activity or admission to an institution."
Privacy Impacts	Privacy impacts are defined as the ways in which a privacy risk could impact the agency, division, program, and the reputation of these three.
Privacy Impact Assessment (PIA)	A PIA is a methodological approach for assessing the privacy aspects of an information system that processes PI.
Privacy Risk	A privacy risk is an aspect of a system and its information that possess a risk to the agency, divisions, or programs and to the individuals whose PI is in the system.
Privacy Threshold Assessment (PTA)	A PTA is an assessment to determine whether a PIA is required by identifying whether a system collects, retains, or otherwise processes PI.

EXECUTIVE SUMMARY

Protecting the privacy of Hoosiers is a key priority for Indiana State Government. As the State's enterprise data agency, the Indiana Management Performance Hub (MPH) assumes a leadership role with respect to data and is responsible guiding Indiana's data innovation initiatives. The MPH fulfills its policymaking and guidance role through the Indiana Office of the Chief Data Officer (OCDO).

To successfully accomplish this priority, the OCDO has promulgated the State of Indiana Information Privacy Policy and offers tools and guidance to ensure that state agencies employ industry-leading privacy standards and protocols as they leverage data. This document is intended to provide Indiana State Government and other data partners with a privacy assessment and roadmap as well as the methodology used to establish these standards and protocols.

One tool created by the OCDO to support this effort is the privacy impact assessment, or PIA. The PIA is intended to provide privacy leaders throughout State government with a baseline understanding of their agency's current privacy posture as defined by recognized industry-leading best practices. By evaluating and scoring potential privacy risks, the PIA offers agencies valuable guidance in the mitigation of those risks throughout the development life cycle of a program or system.

Additionally, PIAs serve several purposes:

- To evaluate risks associated with the collection, maintenance, and dissemination of PI.
- To evaluate the privacy protocols associated with systems and programs to ensure that all information is adequately protected.
- To ensure that Data Processing conforms to applicable legal, regulatory, and policy requirements throughout all stages of a system's development and operation.
- To assure the public that the State of Indiana is implementing and adhering to industry-leading guidance in a manner that considers the sensitivity of the PI it maintains.

In its support of the PIA framework and the methodology outlined in this document, the OCDO seeks to further enable a robust privacy program for the State of Indiana. By implementing the meaningful privacy-preserving procedures outlined in this document, the various agencies of Indiana State Government will more successfully fulfill their mission in service to Hoosiers.

INTRODUCTION

Privacy Vision Statement

It is the policy of the State of Indiana, guided by the OCDO, to ensure that all state agencies with Personal Information Systems, conduct in compliance with industry-leading standards, a PIA and take courses of action based upon that assessment to mitigate privacy risks.

Purpose
The PIA is designed to help Indiana State Government agencies protect PI in order to meet industry-leading privacy standards and guidance.

A PIA is an analysis of how PI is processed:

- to ensure Data Processing conforms to applicable legal, regulatory, and policy requirements regarding privacy;
- to determine the risks and effects of Processing the PI in a Personal Information System; and
- to examine and evaluate protections and alternative methods for Processing PI to mitigate potential privacy risks.

Because Indiana State Government maintains a large volume of PI, individual state agencies must ensure that the appropriate practices and protections are in place and applied in their environments. This has become particularly important as improvements in data sharing technology have allowed information to be more quickly and easily collected, shared, and analyzed.

Scope
The PIA applies to all Personal Information Systems. This may include information that is owned, sent, received, or otherwise processed by an agency.

The PIA applies to relevant agency staff, contractors acting on behalf of agencies, and to other third-party organizations who are granted authorized access to systems or data.

PRIVACY IMPACT ASSESSMENTS

What is a PIA?

A PIA is a methodological approach for assessing the privacy aspects of an information system that processes PI (Wright, 2012). The goal of a PIA is to provide a methodological approach to analyze how PI in an information system is managed (Office of Personnel Management, 2010):

- to ensure that the collection, use, and sharing of the PI conforms to privacy-related legal, regulatory, and policy requirements;
- to determine the privacy risks associated with a system; and
- to evaluate privacy risks and prioritize actions to mitigate the impact of those risks.

While listed above in the “Definitions” section, it is important to restate the meaning of key terms for the sake of clarity. A Personal Information System is defined by the Indiana Fair Information Practices Act (FIPA) as “any recordkeeping process, whether automated or manual, containing personal information and the name, personal number, or other identifying particulars of a data subject.” Ind. Code § 4-1-6-1(a). Further, Personal Information is defined as “any information that describes, locates, or indexes anything about an individual or that affords a basis for inferring personal characteristics about an individual including, but not limited to, the individual's education, financial transactions, medical history, criminal or employment records, finger and voice prints, photographs, or the individual's presence, registration, or membership in an organization or activity or admission to an institution.” Ind. Code § 4-1-6-1(b).

In regard to PIAs and their relationship to PI, they help stakeholders identify and prioritize the privacy risks associated with Personal Information Systems. Furthermore, they ensure that proper policies and procedures are in place to mitigate those privacy risks (Wright & de Hert, 2012). The types of privacy risks of a system can vary from those that are technology specific, such as concerns about information quality, to organizational privacy risks where there are no procedures in place for individuals to request access to their information stored in a system (Spiekermann-Hoff & Oetzel, 2014).

In the United States, PIAs were first introduced and mandated in the 2002 e-Government Act, which stipulated that all Federal agencies were required to conduct a PIA on their systems (Office of Management and Budget, 2003). Since the passage of the e-Government Act, PIAs have evolved and have been adopted by many private sector organizations and companies to assess the privacy risks of their systems (Brautigam, 2012). There has also been considerable attention to PIAs in the academic literature on information privacy (Marx, 2012).

PIA Benefits

Conducting PIAs on Personal Information Systems has many benefits to organizations beyond simply identifying and managing privacy risks and ensuring compliance with relevant information policies and regulations (Wright, 2011). Other benefits include ascertaining the organizational and reputational impacts that privacy risks pose, maintaining a record of an organization's information systems, and gathering feedback on the systems and their business purpose within the organization from the perspective of multiple stakeholders (William & de Hert, 2012). Regarding the stakeholders involved in the PIA process, collaboration is essential between various stakeholders, including data stewards, system subject matter experts, and those responsible for an organization's privacy efforts (Wright, 2012).

PIA Phases

The process for conducting PIAs has been developed and refined at the Federal level (Management and Budget, 2003), by international governments, and in academic literature (Wright, 2012). Based on a review of PIAs in these areas, phases associated with conducting a PIA include:

- Engaging with stakeholders familiar with an organization's systems, including privacy officers, data stewards, and organizational subject matter experts
- Conducting an inventory of systems containing PI
- Developing and implementing a PIA questionnaire that assesses the privacy risks of a system and identifies the impacts those risks might have on the organization
- Identifying which privacy risks to address and developing recommendations for addressing those risks
- Implementation of changes to the system to address the privacy risks
- Development of a system review plan to ensure that changes have in-fact been implemented

PIA Questionnaire

Essential to the PIA process is the development of a PIA questionnaire, as the questionnaire functions as the tool by which systems containing PI are evaluated, and privacy risks are identified and prioritized (Wright, 2011). Based upon recommendations from the e-Government Act and from the literature, such as Wright and de Hert (2012), PIA questionnaires should include descriptions of:

- What PI information the system collects, retains, shares, and analyzes
- How the information in the system is collected
- How the information is used and for what business purposes
- With whom information is shared both within and external to the organization
- Who has access to the system and its information, what permission controls are in place
- What notices or opportunities individuals have to decline to provide or to access their information
- Possible privacy risks and solutions for addressing those risks
- Policies and procedures for ensuring that information is secured

PIA METHODOLOGY

The Privacy Impact Assessment (PIA) methodology and its components are tailored for Indiana State Government based upon a review of PIAs used by Federal agencies and industry. In addition, this methodology incorporates and is informed by PIA best practices from both academic and trade literatures. Effective development, implementation, and remediation of systems based upon a PIA, requires multiple phases and collaboration between various stakeholders across Indiana State Government. Agency PIAs will be overseen by the Agency Privacy Officer (APO) with guidance and support from the State Chief Privacy Officer (CPO).

The State's PIA methodology is comprised of five phases and is similar to the phases in existing Federal PIAs, an example being the PIA from the Office of Personnel Management (Office of Personnel Management, 2010). These five phases include: 1) System's Stakeholder Identification; 2) System Identification; 3) Privacy Impact Assessment; 4) Risk Identification and Prioritization; and 5) PIA and System Review.

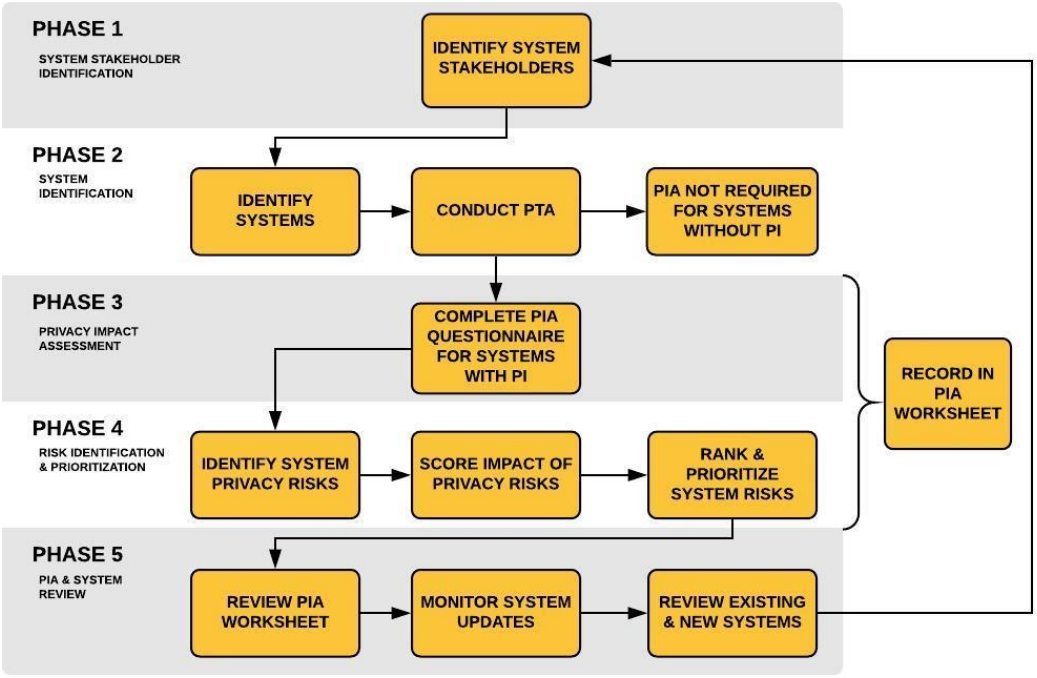


Figure 1. PIA Methodology Phases

Phase 1: Systems' Stakeholder Identification

The first phase involves identifying the agency stakeholders that will be responsible for identification of relevant agency, divisional, and programmatic systems for the PIA. Identifying and engaging a variety of stakeholders in the process is integral to the success of a PIA (Wright & De Hert, 2012). Relevant stakeholders should include the System Owners, Division and Program SMEs, Data Stewards, and the APO. The selection of these stakeholders is based upon recommendations from the Office of Personnel Management (Office of Personnel Management, 2010). In the case that an agency has not yet designated an APO, the agency can work with the CPO to identify an APO, as required in the State of Indiana Information Privacy Policy.[1]

For the PIA process, the agencies' stakeholders will have differing roles and levels of responsibility in the process. These roles include:

- **Agency Privacy Officer** oversees the PIA process, with support from the CPO, by ensuring that the PIA questionnaire and risk assessment worksheet has been completed. The APO will lead or delegate to a knowledgeable privacy professional the completion of the Risk Identification, Impact, and Risk questionnaires after the PIA questionnaire has been completed by the system owner. The APO will further ensure that appropriate recommendations have been made to address identified risks.
- **System Owners** manage the PIA process by identifying agency systems, working with division and program SMEs and data stewards, and completing the PIA questionnaire.
- **Division and Program SMEs** partner with the system owners to identify relevant systems and help complete the PIA questionnaire and risk assessment worksheet by providing support to address the questions related to the business aspects of the systems. These stakeholders also help to identify the business risks associated with the system.
- **Data Stewards** work with system owners to ensure that the questions in the PIA questionnaire and risk assessment worksheet related to the data in the system are accurately recorded. These stakeholders also identify the data risks associated with the system.

Phase 2: System Identification

In this phase, the agencies' System Owners, Data Stewards, and Division and Program SMEs identify relevant systems necessary for the business operations of their agency, divisions, and programs. While it is important to ensure that all State systems adhere to privacy standards, not all systems will require a

[1] https://www.in.gov/mph/files/State-of-Indiana-Information-Privacy-Policy.pdf

PIA. In this phase, prior to conducting a PIA, the stakeholders identify all relevant systems and conduct a Privacy Threshold Assessment (PTA) on those systems. A PTA is an assessment to determine whether a PIA is required by quickly identifying whether a system constitutes a Personal Information System (United States Office of Personnel Management, 2010). The PTA process is a simple step where System Owners work with the Data stewards to examine the system's information to identify whether the system contains PI. If a system contains PI, then a PIA is required. If the system does not contain PI, then a PIA is not required for that system.

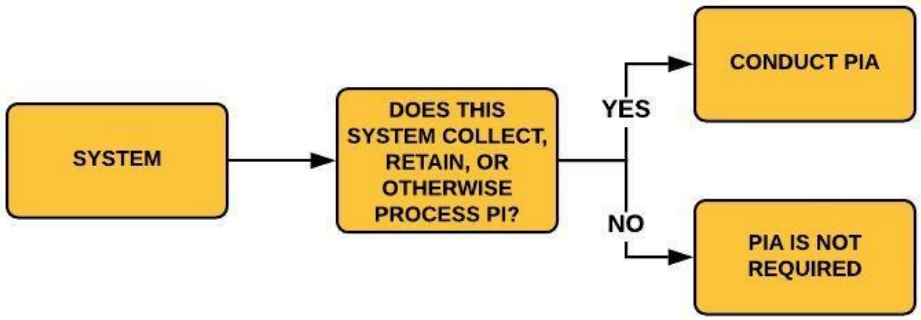


Figure 2. Privacy Threshold Analysis process

Phase 3: Privacy Impact Assessment

This phase focuses on completing the PIA questionnaire, which has been primarily informed by the Indiana Fair Information Practices Act (IC 4-1-6-2 and IC 4-1-6-7) and the U.S. eGovernment Act of 2002 guidance on conducting PIAs (Office of Management and Budget, 2003). Federal PIAs also served as examples in developing the questionnaire, including those from the Office of Personnel Management (Office of Personnel Management, 2010) and the Department of Interior (Department of Interior, 2014). Additionally, the PIA questionnaire has been informed by the European Union's Data Protection Impact Assessment (Wolford, 2020), as well as from academic literature on PIAs (Joyee De & Le Metayer, 2016; Warren et al., 2008; Wright, 2013; Wright & De Hert, 2012; Wright & Raab, 2014).

In addition, these sections and their associated questions (see Appendix 1) have been informed by the Indiana Fair Information Practices Act and the State of Indiana Information Privacy Policy (Cotterill, 2017). For example, the Indiana Fair Information Practices Act requires that State agencies ensure that there are policies and procedures are in place to enable individuals to request access to their information in

State systems (IC 4-6-1-3) and to correct any information that is incorrect in those systems (IC 4-1-6-5). These examples are reflected, respectively, in the table below in sections six and seven.

The table below lists and provides a description of the eight sections that are included in the PIA questionnaire. Each section contains a set of questions, which can be found in Appendix 1. The System Owners work with the Division and Program SMEs and Data Stewards to complete the PIA questionnaire for each agency system identified as containing PI. The responses to the questionnaire are recorded in the PIA Worksheet for each of the systems. The PIA Worksheet is described in further detail in a later section.

Privacy PIA Sections	Section Description
1. Summary of System	Provides an overview of the system, including the system owners and stakeholders, the status of the system, and the reason for which a PIA is being conducted.
2. Description of System's Information	Details the information in the system, how the information is collected, checked for quality, and from what sources. It also identifies legal authorities that allow for the collection of the information.
3. Use of Information	Describes how the information supports the business purpose for the agency, division, or programs.
4. Retention of Information	Explains the retention process and schedule for the system's information.
5. Information Sharing and Disclosure	Discusses the internal and external information sharing policies and procedures, and the legal mechanisms that allow for data sharing.
6. Notice to individuals	States how individuals are notified that their information is being collected and the procedures to which individuals must consent to have their information collected.
7. Access, Redress, and Correction of Information	Outlines the policies and procedures that individuals must follow to access their information and correct any erroneous data about them.
8. Access, Security, and Training	Describes who has access to the system, the protocols in place for granting access, and the training in place to ensure

	that people know how to properly use the system and its information.

Table 1. PIA Sections and Descriptions

Phase 4: Risk Identification and Prioritization

Upon completing the PIA questionnaire in the PIA Worksheet for each of the systems, the APO works with the System Owners and other stakeholders to identify possible privacy risks of the systems and then rate the feasibility of timely addressing the identified privacy risks. Importantly, feasibility scores lasting remediation measures, like long-term administrative or technical enhancement, rather than those that are ad-hoc, like reactive access deprovisioning. Examples of possible information system privacy risks are presented in the table below.

In addition to privacy risks, the APO should determine and rate the potential impacts of those risks. Each privacy risk is rated based upon four impact factors: legal, agency operational, division operational, and reputation. Using the feasibility of addressing the risk scores and privacy impact scores, the APO then ranks and prioritizes the risks to be addressed. This process is described in detail in the PIA Worksheet section of this document.

PIA Sections	Example Privacy Risks
1. Summary of System	Limited support from stakeholders Lack of privacy-minded human resources capacity within the agency
2. Description of System's Information	Collection of unnecessary PI Failure to adhere to relevant legal and agency policies
3. Use of Information	Insufficient mechanisms in place to ensure PI is not inadvertently disclosed Reporting on inaccurate or out-of-date information
4. Retention of Information	Retention of unnecessary PI Lack of approved records retention schedule
5. Information Sharing and Disclosure	Sharing of unnecessary PI

	Unclear policies and procedures of information sharing
6. Notice to individuals	No procedures to notify individuals Inability for individuals to consent
7. Access, Redress, and Correction of Information	Individuals are unable to access their information Individuals cannot correct inaccurate information
8. Access, Security, and Training	System training for users unavailable Absence of clear policies for granting and revoking system access

Table 2. Privacy Risk Examples

Phase 5: PIA and System Review

In this phase, System Owners submit to the APO the completed PIA Worksheet for each of the systems they own. The APO reviews the completed PIA Worksheet and works with System Owners and other agency stakeholders associated with the systems to determine which risks are of the highest priority to address.

The APO then submits the completed PIA Worksheets and the system update recommendations for addressing privacy risks to the CPO. The CPO partners with the APO's to monitor and inform system updates. Once the updates have been made, the APO ensures those are documented and reflected in future PIAs.

On an annual basis, the APO shall oversee an inventory of agency systems to ascertain whether the systems require a PIA. For systems that have previously been subject to the PIA process, the APO may request that another PIA be completed for that system. The APO also works with System Owners to identify any new agency systems that have been developed or procured that would require a PIA.

Other scenarios may trigger the PIA process as well. In such cases, the APO will work with the CPO to determine whether the PIA process is required. Regarding these situations, the e-Government Act of 2002 (Office of Management and Budget, 2003) offers guidance as to when it is appropriate to conduct a PIA, particularly when significant changes are made to a system. Significant changes to a system may include:

- New policies or procedures have been developed that affect how the system handles PI

- Merging of the system's information with information from another system
- Changes to the stakeholder management and ownership of the system
- Modifications to the accessibility and information sharing processes of information in the system
- Alterations to the character of the information in the system, such as the adding of new PI fields or changing previously anonymous information to PI

PIA WORKSHEET

The PIA worksheet is the tool through which state agencies complete the PIA questionnaire for each of the systems requiring a PIA. The PIA questionnaire is not required for systems not containing PI identified in the PTA in Phase 2. The worksheet is modeled from the NIST Privacy Risk Assessment Methodology developed by the National Institute of Standards and Technology (National Institute of Standards and Technology, 2019). The worksheet serves as the output for identifying privacy risks, their potential impact, and ranking and prioritizing each of the risks for remediation. For each of the agency systems that are undergoing a PIA, a new worksheet should be completed. The PIA worksheet contains four questionnaires following the introduction.

Sheet 1: PIA Questionnaire

The first sheet in the PIA Worksheet is the PIA questionnaire, where the System Owners can record their response to each question in the eight sections of the questionnaire. For a list of the questions for each of the eight sections see the table in Appendix 1. When filling out the questions, it is important that the questionnaire is clearly written, detailed, and can be understood by both a technical and non-technical audience. The responses to the questions will be used to complete the rest of the questionnaire. Section 1 of the PIA questionnaire encompasses the PTA. Responses to the PTA questionnaire determine whether the PIA (encompassing Sections 2-8) is required.

Sheet 2: Risk Identification & Feasibility

Based on the responses in the PIA questionnaire, APOs and System Owners identify potential privacy risks of the system. Each identified risk is then rated as to the feasibility of the agency or division in being able to timely address the privacy risk. While it is important to address all privacy risks, certain risks are easier to address than others, and will require fewer organizational resources. This step in the process helps the System Owners identify and prioritize which risks to address.

The scale of rating the feasibility of addressing the privacy risk is 0-5. For risks that would potentially have a low feasibility, that risk is assigned a score of 0-1, moderate feasibility is assigned a score of 2-3, and high feasibility would be given a score of 4-5. When determining the feasibility score, consider the organizational resources (human, financial, and infrastructural) necessary to address the risk, as well as the agency or division's capacity to address the risk given the necessary resources. The figure below provides an example of risk identification and scoring in the Risk Identification questionnaire.

PIA Sections	Possible Privacy Risks	Privacy Risk ID	Feasibility of Addressing Risk
2. Description of System Information	*There are no procedures in place to ensure the quality of PI during data collection*	*2.a*	*3*
	System enables an unnecessary collection of PI	*2.b*	*5*

Figure 3. PIA Worksheet Sheet 2: Privacy Risk Identification and Feasibility of Addressing Risk

Sheet 3: Privacy Impact Rating

The third sheet in the PIA Worksheet focuses on further understanding the impacts that each privacy risk may have if not timely addressed. For each risk, the APO and System Owner first describe the possible impacts of each risk, should it occur. When describing these impacts, it is important to detail the impact of the risks based upon four impact types: legal, agency operational, division operational, and reputation.

- **Legal Impact** – the legal impacts that could arise if a risk is not addressed, such as the legal implications of non-compliance regarding proper management of PI
- **Agency Operational Impact** – how an agency's business operations could be impacted by the privacy risk
- **Division Operational Impact** – how a division's business operations could be impacted by the privacy risk
- **Reputation Impact** – how individuals' perceptions of and trust in the agency, division, or program could be impacted

For each privacy risk, a rating of 0-5 is given to each of the impact types, with 0-1 signifying that the risk has low impact, 2-3 moderate impact, and 4-5 that the risk has the potential for the greatest impact. Determining what score to assign to each impact is described in the table below. The impact types and their ratings have been informed by the Federal Information Processing Standards Publication 199 (National Institute of Standards and Technology, 2004).

Impact Type and Rating	Impact Type Definition
Low Impact (0 – 1)	The potential impact is LOW if the privacy risk could be expected to have limited adverse effects. Limited adverse effects of a privacy risk means that there could be: (i) no legal implications due to the risk; (ii) limited implications on the business

	operations of the agency and divisions; and (iii) little to no impact on the public's perception of and trust in the agency or division.
Moderate Impact (2 – 3)	The potential impact is MODERATE if the privacy risk could be expected to have significant adverse effects. Significant adverse effects of a privacy risk means that there could be: (i) possible legal implications due to the risk; (ii) disruptions to the agency or division's operations where they are able to perform their primary functions, but the effectiveness of the functions are significantly reduced; and (iii) possible implications on the public's perception of and trust in the agency or division.
High Impact (4 – 5)	The potential impact is HIGH if the privacy risk could be expected to have severe adverse effects. Severe adverse effects of a privacy risk means that there could be: (i) numerous legal implications due to the risk; (ii) severe disruptions to the agency or division's operations where they are unable to perform their primary functions, or the effectiveness of the functions are severely reduced; and (iii) severe implications on the public's perception of and trust in the agency or division.

Table 3. Impact Type Ratings and Definitions

Risk is given a Total Privacy Impact rating, by adding up the total for each of the impacts, which can range from 0-20. The figure below provides an example of two privacy risks and their impact ratings.

PIA Sections	Privacy Risk ID	Privacy Risks	Describe Possible Impacts of Risk	Privacy Impact Ratings, Should the Risk Occur				Total Privacy Impact
				Legal Impact	Division Operational Impact	Agency Operational Impact	Reputation Impact	
2. Description of System Information	*2.a*	*There are no procedures in place to ensure the quality of PI during data collection.*	*Without data quality procedures, the quality of the reports created using the information could be inaccurate.*	*0*	*4*	*3*	*5*	***12***

	2.b	*System enables an unnecessary collection of PI.*	*Unnecessary collection of PI could result in the division violating regulations and putting the division at risk of litigation.*	*5*	*5*	*4*	*4*	***18***

Figure 4. PIA Worksheet Sheet 3: Privacy Risk Impact Rating

Sheet 4: Privacy Risk Prioritization

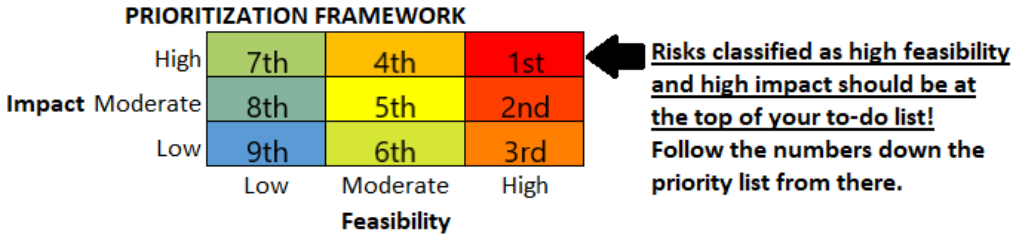
In the final sheet, a color scale is displayed for each risk based upon the Feasibility of Addressing Risk score and Total Privacy Impact score determined in the previous two sheets. This scale can be used by the system's stakeholders to determine which of the risks to prioritize and take actions to mitigate those risks.

For each privacy risk, a color shade will be assigned using a hot-cold color scale. The sheet displays the privacy risks, the feasibility of addressing those risks, and the impact those risks could have on your agency, should they occur. The feasibility rating from Tab 3. 'Risk Identification' is multiplied by four (4) and displayed on this tab to enable a like comparison with the total privacy impact rating. A higher feasibility rating indicates that the risk can more easily be addressed. A higher impact rating illustrates the degree to which the risk could negatively affect your agency. Taken together, the ratings indicate the urgency with which a given risk should be addressed.

A hot-cold scale is used for each rating, with blue indicating 'low', yellow indicating 'moderate', and red indicating 'high'. Risks should be prioritized for remediation based first upon the feasibility score and second upon the impact. For instance, the examples below in rows 11 and 12 show a moderate feasibility with moderate impact in 2.a and a high feasibility with high impact in 2.b. 2.b is both easier to address and a more impactful use of resources to address—it should be prioritized.

The suggested prioritization framework is as follows:

1) high-high; 2) high-moderate; 3) high-low; 4) moderate-high; 5) moderate-moderate; 6) moderate-low; 7) low-high; 8) low-moderate; 9) low-low.



The color scale is as follows:

The figure below provides an example of this section of the worksheet.

PIA Section	Privacy Risk ID	Privacy Risks	Feasibility of Addressing Risk	Total Privacy Impact
2. Description of System Information	*2.a*	*There are no procedures in place to ensure the quality of PI during data collection*	***12***	***12***
	2.b	*System enables an unncessary collection of PI*	***20***	***18***

Figure 5. PIA Worksheet Sheet 4: Privacy Risk Prioritization

REFERENCES

Brautigam, T. (2012). PIA: Cornerstone of privacy compliance in Nokia. In. D. Wright & P. de Hert (Eds.), *Privacy Impact Assessment* (pp. 253 – 274). Springer Science & Business Media.

Cotterill, T. (2017). *State of Indiana Information Privacy Policy.* https://www.in.gov/mph/files/State-of-Indiana-Information-Privacy-Policy.pdf

De, S. J., & Le Métayer, D. (2016). PRIAM: a privacy risk analysis methodology. In *Data Privacy Management and Security Assurance* (pp. 221-229). Springer, Cham.

Department of Energy (2010, June). *Best practices: Elements of a federal privacy program.* https://www.energy.gov/sites/prod/files/Elements%20of%20a%20Federal%20Privacy%20Program%20v1.0_June2010%20Final.pdf

Department of the Interior (2014, September 30). *Privacy impact assessment guide.* https://www.doi.gov/sites/doi.gov/files/uploads/DOI-PIA-Guide-09-30-2014.pdf

GDPR European Union (2020). *Data protection impact assessment (GDPR): How to conduct a data protection impact assessment.* https://gdpr.eu/data-protection-impact-assessment-template/

Information and Privacy Commissioner of Ontario (2015, May 19). *Planning for success: Privacy impact assessment guide.* https://www.ipc.on.ca/resource/planning-for-success-privacy-impact-assessment-guide/

Marx, G. T. (2012). Foreword: Privacy is not quite like the weather. In. D. Wright & P. de Hert (Eds.), *Privacy Impact Assessment* (pp. v-xiv). Springer Science & Business Media.

National Institute of Standards and Technology (2004, February). Federal information processing standards publication 199: Standards for security categorization of federal information and information systems. https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.199.pdf

National Institute of Standards and Technology (2019, September 19). *Risk assessment tools.* https://www.nist.gov/itl/applied-cybersecurity/privacy-engineering/collaboration-space/browse/risk-assessment-tools

Oetzel, M. C., & Spiekermann, S. (2014). A systematic methodology for privacy impact assessments: a design science approach. *European Journal of Information Systems*, *23*(2), 126-150.

Office of Personnel Management (2010, April 22). *Privacy impact assessment (PIA) guide.* https://www.opm.gov/information-management/privacy-policy/privacy-references/piaguide.pdf

Office of Management and Budget (2003, September 26). *OMB guidance for implementing the privacy and provisions of the e-Government Act of 2002.* https://www.whitehouse.gov/wp-content/uploads/2017/11/203-M-03-22-OMB-Guidance-for-Implementing-the-Privacy-Provisions-of-the-E-Government-Act-of-2002-1.pdf

Securities and Exchange Commission (2007). *Privacy impact assessment (PIA) guide.* https://www.sec.gov/about/privacy/piaguide.pdf

Warren, A., Bayley, R., Bennett, C., Charlesworth, A., Clarke, R., & Oppenheim, C. (2008). Privacy Impact Assessments: International experience as a basis for UK Guidance. *Computer Law & Security Review*, *24*(3), 233-242.

Wright, D. (2011). Should privacy impact assessments be mandatory?. *Communications of the ACM*, *54*(8), 121-131.

Wright, D. (2012). The state of the art in privacy impact assessment. *Computer Law & Security Review*, *28*(1), 54-61.

Wright, D. (2013). Making privacy impact assessment more effective. *The Information Society*, *29*(5), 307-315.

Wright, D., & de Hert, P. (Eds.). (2012). *Privacy Impact Assessment* (Vol. 6). Springer Science & Business Media.

Wright, D., & Raab, C. (2014). Privacy principles, risks and harms. *International Review of Law, Computers & Technology*, *28*(3), 277-298.

APPENDICES

APPENDIX 1: PIA Questionnaire

PIA Sections	PIA Section Questions
1. Summary of System Provides an overview of the system, including the system owners and stakeholders, the status of the system, and the reason for which a PIA is being conducted.	• Name of the information system • Name of agency for system • Name of agency division for system • Name of agency program for system • Name System Owner • Name of system Data Steward • Name of Division and Program SME of system • Name of Agency Privacy Officer • Name of the contractors or vendors associated with the system • Status of system (current, new, etc.) • Date of system's last PIA • Description of the system • Business purpose of the system • Does the system collect, retain, or otherwise process PI?
2. Description of System's Information Details the information in the system, how the information is collected and checked for quality, and from what sources the information comes from. It also includes the policies that allow for the collection of the information.	• What personal information is collected, retained, or otherwise processed? • Does the system collect, retain, or otherwise process confidential information? • If so, what confidential information is collected, retained, or otherwise processed in the system? • If so, what is the statute, rule, or other obligation that makes this information confidential? • What are the sources of information? • Does the system collect information to the greatest extent possible from the data subject directly? • Does the system capture information regarding the data subjects' political or religious beliefs?

	• Why is the information being collected, retained, or otherwise processed? • How is the information collected? • What technologies are used to collect the information? • What legal authorities, arrangements, and agreements define the collection of information? • If other was selected in previous question, please list what those are? • Where is the information in the system stored? • If other was answered in the previous question and if the information is not stored on-premise by the Indiana Office of Technology, are the State of Indiana Additional Terms and Conditions for Cloud Service Engagements incorporated into the contract with the vendor storing the information? • Does the system have a data dictionary or a description of the system's metadata? • Is the use of personal information both relevant and necessary to the purpose for which the system was designed?
3. Use of Information Describes how the information supports the business purpose for the agency, division, or programs. In addition to the types of reports and analyses conducted using the information.	• How is the information in the system used to support the division's business purpose? • What types of tools are used to analyze data and what type of data are produced? • Does the system leverage artificial intelligence (AI) and/or machine learning (ML) to process data? • If the system leverages AI and/or ML to process data, how is the result of that processing used? • If the system leverages AI and/or ML to process data, is the NIST AI Risk Management Framework applied to address risks of AI systems? • Does the system use commercial or publicly available data? • If the system uses commercial or publicly available data, how is that used? • Is the information in the system duplicated to create new records? • If so, what is the purpose for creating new records?

	• How is data retrieved from the system? • What are the physical locations from where the system is accessed by users? • How does the agency ensure consistent use of the system across the different physical locations? • What reports are created using the data from the system? • How is information checked for accuracy?
4. Retention of Information Explains the retention process and schedule for the system's information.	• What information is retained? • How long is the information retained? • What are the procedures for identification and disposition of the data at the end of the retention period? • What is the Record Series Number assigned by the Indiana Archives and Records Administration?
5. Information Sharing and Disclosure Discusses how information is shared within the agency, to other agencies, and to organizations external to the state, and the information sharing policies, procedures, and legal mechanisms that allow for data sharing.	• With which divisions internal to the agency is information shared • What information is shared with other divisions and for what purpose? • How is the information shared with other divisions in the agency? • With which other agencies is information shared? • What information is shared with other agencies and for what purpose? • How is the information shared with other agencies? • What legal allowances are leveraged to enable the exchange of information with other State agencies? • If other was selected in the previous question, please list what those are. • With which organizations external to the State is information shared? • What information is shared with organizations external to the State and for what purpose? • How is the information shared with organizations external to the State? • What legal allowances are leveraged to enable the exchange of information with organizations external to the State?

	• If other was selected in previous questions, please list what those are. • How is shared information destroyed upon expiration of the reported sharing periods?
6. Notice to individuals States how individuals are notified that their information is collected and the procedures to which individuals must consent to have their information collected.	• Is notice provided to the individual before collection of information? • Do individuals have the right to decline to provide information? • Do individuals have the right to consent to particular uses of information?
7. Access, Redress, and Correction of Information Outlines the policies and procedures regarding how individuals access their information and correct any erroneous data about them.	• What are the procedures that allow individuals to gain access to their information? • What are the procedures for individuals to correct inaccurate or erroneous information? • How are individuals notified of the procedures for correcting their information?
8. Access, Security, and Training Describes who has access to the system, the protocols in place for granting access, and the training set up to ensure that people know how to properly use the system and its information.	• What procedures are in place to determine which users may access the system? • What privacy trainings are available specific to the system or program? • Which user group(s) will have access to the system? • Are contractors involved with the design, development, maintenance, and use of the system? • If yes, which contractors are involved with the system and what is their role? • What auditing measures/controls and technical safeguards are in place to prevent misuse (e.g., unauthorized browsing) of data? • How is personal information secured? • Who is responsible for ensuring that personal information is secure? • What oversight mechanisms are in place to address privacy and security risks to the personal information?