Introduction to the Design Process Standard

The IOPD is still drafting this introductory paragraph on the standard. Commentors are asked to suggest important introductory information necessary to guide the audience in reading and using the standard.

Elements of the Standard

Component: The constituent elements that an organization must have. What are we talking about? Are we talking about dogs, or are we talking about a cat? Just a high-level descriptor of this particular Component of the standard. [Disambiguation: this is the Component of the ***standard***, not a component of a system.]

Phases: Refers to the phases of the Lifecycle: Ideation, Development, and Deployment.

Objective: One to three sentences describing why this Component is important. What are we trying to achieve with this Component? This will help determine whether what the organization puts forward is sufficient. For instance, a dog provides companionship, alerts to dangers, and protects the owner from danger.

Description: This is the detailed description of the Component. The Component might be a dog, and the description explains that a dog is a furry animal with four legs and a tail that wags, that responds to commands and eats dog food. A dog is not a cat, so maybe the description includes what it is not, in order to distinguish it. In other words, the description describes the criteria that the organization must meet to be able to claim it has this Component in place.

Implementing Guidance: This will be a description of common pitfalls, or clarification as to how the organization actually goes about executing this Component. For instance, you need to ensure the dog is sufficiently big and scary to ward off dangers, but still cuddly and soft.

Evidence: What evidence will the organization need to present to show it has this Component in place? This evidence should be practical, but thorough. For example, a video must be presented showing the dog playing with kids and barking/growling at the letter carrier who ran away in fear.

Evaluation: How will the evidence be measured and judged to be sufficient and effective? The video must show at least two instances of each.

Definitions

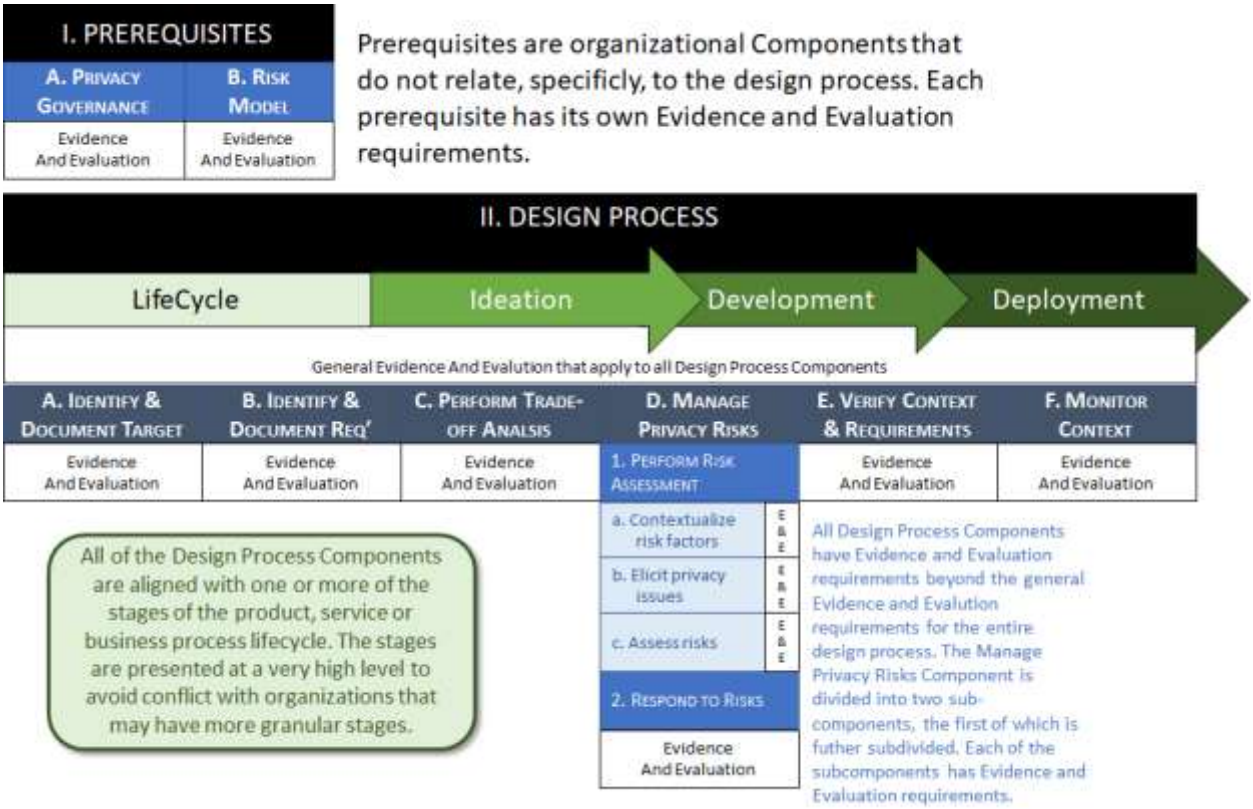
- **System** - The product, service, or business process, or an element of a product, service, or business process.
- **Target System** - The system being designed, developed, or deployed as part of the process. The target system is distinguished from a general system.
- **Risk Model** - A representation that elaborates key terms and abstract factors that contribute to or negate privacy harms. (see NIST definition)
- **Privacy Harm** - A negative consequence that falls under the umbrella of privacy.
- **Privacy Issue** - The existence of a threat, vulnerability or harm that creates risk.
- **Risk Factor** - An element which affects, influences, or determines the likelihood or severity of privacy harm. Examples include: the number or types of at-risk individuals, their roles in the target system, or the data about them.
- **Risk** - A measure of likelihood and severity of privacy harm using the Risk Factors under a particular Risk Model.
- **Risk Appetite** - How much privacy risk the organization is willing to allow affected entities to incur through its systems.
- **Risk Tolerance** - How much variance from its stated Risk Appetite the organization is willing to tolerate.
- **Context** - The particularized elements that contribute to or negate privacy harms from a target system, aligned to the Risk Factors making up the organization's Risk Model. For instance, at-risk individuals (abstract factor) ⇒ employees (particularized element)
- **Residual Risk** - A measure of risk remaining after a change in the context, such as applying controls.
- **Approach** - A method, process, or procedure to accomplish a goal.
- **Lifecycle** - While business activity around a system may be broken down into many lifecycle phases, this standard uses three high level ones. The demarcation points between each phase may not necessarily be clean.
    - **Ideation** - The phase in which the organization is trying to investigate and draw the contours of the desired system. Ideation generally answers the question of what is being designed (e.g. "a service providing X")
    - **Development** - The phase in which the organization is trying to actually design and build the system. Development generally answers the question of how the organization plans to provide the service, product, or business process (e.g. "using a mobile app accessing APIs on a server running in a cloud").
    - **Deployment** - The phase in which the organization actually makes available the system for use. This phase also includes ongoing use and operation of the product, service, or business process.

IOPD Design Process Standard

Components Outline

I. Prerequisites
    A. Privacy Governance
    B. Risk Model
II. Design Process
    A. Identify and document the target system
    B. Identify and document requirements
    C. Perform trade-off analysis
    D. Manage privacy risks
        1. Perform Risk Assessment
            a) Contextualize risk factors
            b) Elicit privacy issues
            c) Assess risks
        2. Respond to Risks
    E. Verify the target system context and requirements
    F. Monitor context

The following chart illustrates the major organizational structure of the Standard. The Prerequisites are not associated with a particular lifecycle Phase. The Phases are explained at the beginning of the Design Process Components section.



I. Prerequisites

Component: I.A. Privacy Governance
Phase: N/A
Objective: To have in place the governance to successfully integrate privacy into the design of systems.

Description: The organization must have a governance function in place to manage privacy in the ideation, development, and deployment of systems. This governance function must include:

- Policies, standards, and procedures
- Human resources with appropriate roles and responsibilities
- Training for those resources commensurate with their role and responsibilities
- Ownership or accountability for each of the design process points
- A set of privacy values in line with organizational missions and objectives
- A control framework identifying the source of controls, regulatory guidance, and company policies or standards used to mitigate privacy risks

A robust set of tools for common scenarios to mitigate possible privacy risks in the risk model.

Implementing Guidance: The organization should leverage best industry practices, common privacy program and project management processes, or a recognized privacy framework in organizing and creating their policies and procedures. The organization should engage stakeholders to ensure success.

Evidence:

- **Documentation:** Policies, standards, and procedures include HR, accountability and governance, risks and controls, and training that relates to the organization's design process. Documentation further includes approvals, reviews, and internal communications.
- **Human Resources:** Job descriptions and required qualifications
- **Training:** Design training curriculum and content, training records, and training feedback or results

Accountability: Organization charts with roles and responsibilities related to the design process

Evaluation: The Assessor will examine the evidence to determine if:

- The organization's policies, standards, and procedures have been documented, approved, reviewed, and communicated to the organization's staff.
- The organization clearly defines and articulates job descriptions and required professional qualifications for all personnel in the design process.
- The organization's training is mandatory, addresses knowledge and skills required to perform roles and responsibilities in the design process, and requires individuals to complete assessments to demonstrate their proof of comprehension relevant to their job function.
- The organization has a well-defined reporting structure, clearly identified executive management oversight, and business process owners for governance and accountability responsibilities in the design process.

The organization utilizes standardized privacy risks, controls, and a requirements library/repository containing a collection of safeguards, countermeasures, techniques, and processes which can be leveraged for risks identified in the risk model.

Component: I.B. Risk Model
Phase: N/A

Objective: To conduct risk assessments in a consistent and structured manner. Having a defined risk model (or process) enables the organization to consistently evaluate risk posture across different systems as well as the same systems over time.

Description: The organization must incorporate either (a) one or more privacy risk models as a basis for privacy risk analysis, (b) a process by which system-specific privacy risk models are developed as a basis for privacy risk analysis, or (c) a combination of (a) and (b).

A. A privacy risk model or model development process must address each of:
    A. Threats
    B. Vulnerabilities
    C. Adverse consequences
    D. Likelihood
    E. Severity of impact
B. The organization must have explicitly established an enterprise privacy risk appetite and privacy risk tolerance.

NOTE: Measures of likelihood and severity of impact could include justification for use of a constant value. For instance, an organization may wish to assume that threats are going to happen and ignore a qualitative measure of likelihood, focusing their attention on measuring the severity of impact.

Implementing Guidance: The organization's risk model must at a minimum focus on risks to individuals affected by the system**.** The risk model may also include organizational risks, group risks, and societal risks.

The risk model is a generic model to be applied to each of the target systems. This application is done at the "Elicit privacy issues" Sub-Component stage of the risk assessment. In other words, the risk model might consider the risk of spamming as one of concern to the organization. During the risk assessment, the organization would identify that a particular system had the risk of spamming because it allowed people to send messages to other users of the system.

Evidence:

- Documentation of the privacy risk model and/or system-specific risk model development process. Process documentation may exist independently or be embedded in a relevant tool. In either case, the documentation should define and/or describe the process for defining relevant privacy risk models. It should also describe how the models are to be used.
- Documentation of the organizational privacy risk tolerance and appetite consistent with the risk model and/or documentation of a process for identifying organizational privacy risk tolerance and appetite.

Evaluation: The Assessor will examine the evidence to determine if the risk model or risk model development process is sufficiently objective to be repeatable, and that the risk model covers:

- Threats
- Vulnerabilities
- Adverse consequences to individuals, at a minimum
- Quantitative or qualitative measures of the likelihood or frequency of threats, vulnerabilities, and consequences
- Quantitative or qualitative measures of the magnitude or impact of consequences

The Assessor will examine the risk tolerance and appetite to determine if it is consistent with the risk model or if the process for identifying organizational privacy risk tolerance and appetite will sufficiently match the risk model's quantitative or qualitative measurements.

158
159

II. Design Process

160
161
162

General Evidence Requirements for All Lifecycle Components:

- The organization must have a documented policy, standard, or procedure which addresses the elements of the Component. Such policies, standards, or procedures may have exception processes which allow escalation of decisions outside of the normal procedure.
- The organization must have evidence for the target system(s) demonstrating compliance with the documented policy, standard, or procedure and which addresses the elements in the Description of the Component.

General Evaluation for All Components:

The Assessor will examine the evidence and determine if:

- each element of the Component is sufficiently addressed in the documented policy, standard, or procedure.
- the policy, standard, or procedure addressing the Component is sufficiently documented to be repeatable with similar results (e.g., objectivity)
- the minimal requirements of the policy, standard, or procedure meet the objective of the Component.

The Assessor will select a target system and examine the evidence to determine if:

- the organization followed the documented policies, standards, and procedures related to the Component.
- The Assessor will review that the documentation for the selected target system addresses each of the elements of the Description of the Component.

163
164
165
166

Component: II.A. Identify and document the Target System
Phase: Ideation and development
Objective: To bound the analysis. Scoping the target system helps organizations avoid missing important system components and avoid over-analysis. The objective of documentation is to ensure the organization has sufficient detail and agreement as to what is the target system.
Description: The organization must describe the system in a high level use case with sufficient detail to bound analysis. The high level use case should include: ● What is the purpose/goal/objective of the system ● What are the intended components of the system ● How will the system be used ● Who will use the system ● Whether and what kinds of personal information the system will process
Implementing Guidance: The high level use case must be documented in a way that is useful to those in the organization who are working on the system. Documentation can include, for example: ● Product specifications ● Architectural diagrams ● Data Flow diagrams ● Data registers ● Business Requirements Document [BRD] ● Business Case documents ● User stories
Evidence: See General Evidence II.X
Evaluation: See General Evaluation II.X

The Assessor will review the evidence of the target system to determine if the high level use case is documented in a way that is useful to those in the organization who are working on the system.

167
168

Component: II.B. Identify and document requirements (Functional / Non-functional)

Phase: Ideation and development

Objective: To explicitly articulate the objectives and desired attributes that must be satisfied to guide development and serve as the basis for verification activities to show proof of compliance with requirements. Doing this forces systematic consideration of what the system aims to achieve and how it intends to achieve it. The objective includes being able to resolve tensions between requirements. Additionally, explicitly stating requirements facilitates risk management choices.

Description: The organization must have a policy, standard, or procedure to explicitly define and document functional and non-functional requirements for target systems. Requirements may be enterprise wide or system-specific. Documentation of requirements should be made available to others working on the system.

Implementing Guidance: Functional requirements relate to those elements that directly support the system's purposes or goals. Non-functional requirements (also known as quality attributes) relate to crosscutting concerns that do not directly contribute to achieving the system's purposes or goals. Privacy is an example of a quality attribute, as are security, usability, and accessibility.

The organization should establish requirements in two distinct ways: baseline and system-specific.

- Baseline requirements are a standard set of requirements that every system must consider and satisfy, as appropriate. Not every baseline requirement will be equally applicable to every system. Therefore, each requirement must be assessed for applicability and decisions to exclude or tailor particular baseline requirements should be justified. For privacy, baseline requirements tend to be best (but not exclusively) suited to ensuring that systems implement non-functional requirements that address compliance obligations and organizational privacy values.
- System-specific requirements are those requirements that derive from the objectives of a particular system. A key method of identifying non-functional system-specific privacy requirements is to perform a privacy risk analysis of the system's functional requirements. Decisions to mitigate specific risks will yield system-specific privacy requirements. Functional privacy requirements, owing to their nature, will tend to be identified through the larger process of system requirements definition.

Requirements are the what, not the how.

By way of example, a baseline privacy requirement is that systems obtain individual consent for marketing communications (derived from relevant laws in the jurisdictions in which the organization operates). A system-specific requirement is that a specific system sends an initial email to an individual opting in to marketing communications to confirm their selection before being added to the communications list (i.e., double opt-in).

Evidence: Because baseline requirements are not strictly necessary, yet highly advised, evidence of them is mandatory only if the organization claims they are employed, though for most organizations they probably are used. In all cases, though, evidence of system-specific requirements are necessary.

- Baseline requirements: The organization must demonstrate how they are documented. This could take the form of literal documents or the contents of a requirements repository. A requirements repository could take the form of a dedicated database or a component of a broader development tool. The organization must also have related process documentation governing the maintenance and use of the baseline requirements.
- System-specific requirements: The organization must provide documentation of how system-specific requirements are derived as part of their system life cycle activities.

Evaluation: If the organization uses baseline requirements, the Assessor will review the process documentation to ensure it governs the creation and use of baseline requirements. The Assessor will review a sampling, selected by the Assessor, of baseline requirements from any requirements repository used by the organization.

The Assessor will review the documentation on how system-specific requirements are derived. The Assessor will review a sampling, selected by the Assessor, of system-specific requirements for the target system selected by the Assessor for review.

Measured against the meta-document describing the necessary requirements elements. Look at documents on how they define requirements, does what they’ve provide meet the

Are the processes designed appropriately?
Are they operating effectively?

Document what you do, do what you document

169
170
171

Component: II.C. Perform trade-off analysis

Phase: Ideation and Development

Objective: To ensure trade-offs are explicitly identified and resolved, avoiding informal or implicit resolutions that may turn out to be problematic and will likely be undocumented (thereby frustrating any attempt at post hoc reconstruction, should the need arise).

Description: A trade-off analysis is:

- Identification of decision points during ideation or development
- Articulation of available options
- Identification of competing qualities/priorities exhibited by available options
- Comparison of the options using the qualities/priorities against system requirements
- Determination of acceptable design

Documentation of the trade-off analysis should include both the decisions and justifications.

Implementing Guidance: Trade-off analysis is the responsibility of the owner of the system. The owner should designate people with sufficient understanding of the design space to make decisions, and include input from stakeholders.

Trade-off analysis is premised on the existence of plausible design alternatives of sufficient granularity to support systematic comparisons. It therefore must be linked appropriately to the project life cycle. However, ultimately it is a form of decision analysis.

A. Specific methods of performing the analysis should be employed such that the analysis is systematic. Methods employed in systems engineering include, but are not limited to:
    1. Pros/cons comparison
    2. Influence diagrams
    3. Decision trees
    4. Analytic Hierarchy Process
    5. Borda counting
B. The results of a trade-off analysis should be documented in some way, though the degree of formality can vary. It is important that the documentation, irrespective of its form, be retained and accessible to enable trade-off decisions to be revisited if necessary.

Companies may conduct trade-off analysis for common scenarios which are applied across multiple designs.These analyses may be incorporated into design standards.

Evidence:

- The organization must provide documentation demonstrating provision for trade-off analysis within the organization's life cycle processes, including prescribed or

suggested methods. Such documentation may have an exception process which allows escalation of decisions outside of the normal trade-off process.
- The organization must have illustrative samples of the results of trade-off analyses performed.

For design standards, the organization must provide documentation of trade-off analysis done in the development of the standards, or justification for design decisions made without a trade-off analysis.

Evaluation:

The Assessor will review the minimal requirements of the trade-off analysis process to ensure it meets the Objective of the Component, namely requiring the organization, regardless of formality, to:

- explicitly identify decision opportunities in the design that have multiple potentially conflicting objectives, attributes, and/or constraints;
- resolves those decisions; and
- document the decisions and justifications.

The illustrative sample(s), chosen by the Assessor, must show the organization following the documented process.

172
173

Component: II.D. Manage privacy risks
Phase: Ideation, Development and Deployment
Objective: To achieve an acceptable level of privacy risk

174
175

Component: II.D.1. Perform risk assessment
Phase: Ideation, Development and Deployment
Objective: To understand the level of risk involved

176
177

Sub-Component: II.D.1.a. Contextualize risk factors
Objective: To align the context of the target system to the factors in the risk model. This allows for privacy risk assessment using the organization’s risk model.

Description: The organization identifies and documents the context surrounding the target system. The contextual elements examined must correspond to the factors in the risk model that contribute to privacy risk. Some examples of corresponding context to risk factor include: a factor of individuals at risk, in a particular target system context might be employees, data might be contextualized as payroll, schedule and pay rates, threat actors might be contextualized as managers or other employees, and controls might be contextualized as data is encrypted using AES 256.
Implementing Guidance: The organization should look at each factor that contributes to risk within the risk model and identify the particularized value(s) for those factors. Organizations should formally capture those values and make them available to the person conducting the risk assessment. Values should be objectively determined and sourced or, when based on subjective considerations, the rationale should be explicitly described. Justifications for exclusion of certain values, in contravention of the risk model, should be provided.
Evidence: The organization identifies the portions of their risk assessment process which contextualize the factors of the risk model. The organization has documented the values for contextual factors of the target systems.
Evaluation: See General Evaluation The Assessor reviews selected, by the Assessor, values for contextual factors for selected, by the Assessor, target systems.

178

Sub-Component: II.D.1.b. Elicit privacy issues (using the target system documentation and context)
Objective: To identify potential privacy issues in (the current version of) the target system at the earliest opportunity prior to deployment to reduce costs associated with mitigations.
Description: The organization, through a systematic process, identifies and documents the privacy threats, vulnerabilities, and consequences (using the organization or system-specific risk model) that can occur in the target system.
Implementing Guidance: The organization has a systematic threat modeling approach in place to identify privacy issues for each target system. The risk model used for this issue elicitation exercise will determine the focus and thus coverage of the analysis. The organization should capture any assumptions made in the course of the elicitation exercise.
Evidence: The organization has documented the systematic approach being applied. The organization has documented identified issues in the target system.

Evaluation: The Assessor will determine if the organization's approach to issue elicitation is sufficiently systematic to comprehensively identify all threats, vulnerabilities, and consequences resulting from the organization or system-specific risk model, and that the approach can be consistently applied. The Assessor will review identified issues in the target system to ensure all threats, vulnerabilities, and consequences were elicited.

179
180
181

Component: II.D.1.c. Assess risks
Objective: To determine which privacy risks exceed organizational tolerance and appetite.
Description: Using the identified privacy issues, the organization performs an assessment to measure the privacy risks introduced by the target system. Risks are compared to organizational tolerance to identify unacceptable risks in need of mitigation.
Implementing Guidance: Both quantitative and qualitative measurements of risk are acceptable, but there should be objective criteria for measurements or estimation. Where subjective determination is allowed, the organization must provide guidance on how to make that determination as well as justification for using a subjective determination in lieu of objective criteria. Risk and risk tolerance may be viewed in light of countervailing benefits to the affected individuals or society. The risk assessment may take into account existing and documented controls and mitigations. The risk assessment must incorporate the context in which the target system operates. Risk assessments need not always be performed in the context of a specific system and risks may be assessed generally with mitigations introduced through standards or baseline requirements. For example, the security risks of unauthorized access of transmitted data may be mitigated through encryption. An organization need not carry out a risk assessment on every data transmission, provided the mitigation is applied and documented.
Evidence: The organization must have a documented approach for performing risk assessments.
Evaluation: The risk assessment approach will be reviewed for objectivity and ability to be consistently applied where subjective measures are used.

182
183

Component: II.D.2. Respond to risk
Objective: To situate privacy risks within acceptable organizational tolerance.

Description: If privacy risks exceed organizational tolerance, the organization has two options: lower the privacy risks or increase the organization's privacy risk tolerance. While the former is preferred, the latter is an option. The most common way to reduce privacy risk is through the introduction of technical or administrative controls that change the context of analysis. However, not all context changes will be in the form of controls. For instance, deciding not to provide your service to minors would be an example of a context change that would increase the likelihood that your service is used by individuals who might be more mature and able to understand the inherent risks of using the service.

Where controls are used to mitigate risks, they should be designed, developed, or deployed, as appropriate, to sufficiently reduce the risks. A residual risk assessment will demonstrate that reduction.

Implementing Guidance: The organization must have an approach for reviewing contextual changes (such as control selection) to mitigate privacy risks. While context changes need not be wholly objective, the organization should be able to justify why the changes were made and why others were not chosen. This is even more important where context changes were not made and the organizational risk tolerance was expanded to accommodate identified privacy risks. In selecting technical or organizational controls, a framework, such as the Hoepman Privacy Design Strategies and Tactics or the NIST control set, can be leveraged to ensure a comprehensive set of controls are at the organization's disposal.

Evidence: The organization must provide a documented approach for identifying controls to mitigate privacy risks.

The control selection must include justification for why certain controls were chosen and not others. The organization should document the selected controls and mitigations and keep track of the rationale for the selection when trade-off decisions are made.

Evaluation: The proffered approach must be able to mitigate all risk factors as part of the privacy risk model.

184
185
186

Component: II.E. Verify the target system context and requirements

Phase: Development and Deployment

Objective: To ensure that the target system assumptions are correct and the target system functions as expected in the intended environment.

Description: Using assumptions about context, requirements, and controls, identified in the Ideation phase and employed in the design process, the organization must review whether those assumptions, requirements, and controls were inaccurate, incomplete, or ineffective.

Implementing Guidance: The organization's procedures should include steps for reviewing assumptions about the target system context, requirements, and controls post-assessment. For instance, an assumption that only customer data would be included in a system might prove false when customers started uploading pictures of relatives, necessitating the need to conduct an assessment of privacy risks for non-customers.

Evidence: See General Evidence

Evaluation: See General Evaluation

187
188

Component: II.F. Monitor context

Phase: Deployment

Objective: To ensure post deployment context does not vitiate the risk assessment and decisions made, requiring re-evaluation.

Description: Monitor, at least,

- differences between expectation of use and actual use
- changes to the target system,
- changes to the organization,
- changes to the business environment,
- changes to internal business functions, and
- changes legislation, policies, directives, regulations, standards, and social norms.

I. The organization identifies and documents the context for monitoring changes to the target system.
    A. The organization must have policies and procedures for verifying that all privacy requirements have been implemented.
    B. The organization must have procedures for regularly conducting security and privacy verification of the target system to confirm that the controls continue operating effectively. The organization remediates any non-compliant privacy controls or security vulnerabilities.

II. Organization: The organization identifies and documents the context for monitoring changes to the organization that may alter the risk assessment of the target system. Specifically:
    A. The organization must have procedures for monitoring the organization's business strategy, privacy management framework, and risk management priorities.

B. The organization must have procedures for monitoring the organization's merger and acquisition activity or expansion of products and services to another country or region.

III. Business Environment. The organization identifies and documents the context for monitoring changes to business processes, information processes, and system environments and infrastructures that may alter privacy requirements, and confirms that the privacy controls selected continue to be effective.

A. The organization must have procedures for regularly conducting privacy vulnerability assessments for products and services. The organization's exposure to privacy vulnerabilities are evaluated and appropriate measures are taken to address the associated risk.

B. The organization must have procedures for when the system environment or infrastructure is changed; for example, on-site versus cloud. Products and services must be reviewed and tested to ensure there is no adverse impact on privacy.

C. The organization must have procedures for when products, services, or processes are outsourced, in order to evaluate the privacy risks and ensure that the privacy controls selected continue to be effective.

D. The organization must have procedures established for a quick, effective, and orderly response to privacy incidents.

E. The organization must have procedures to monitor all privacy relevant legislative laws and regulations, and explicitly identify and document its method of compliance with these laws and regulations.

Implementing Guidance: The organization must define and apply documented policies and procedures for systematically monitoring changes when there is a change to the existing system, organization, or business environment and/or internal business functions, in order to ensure that privacy risks are measured, analyzed, and mitigated. The organization must retain documentation to serve as evidence of compliance, including remediation plans to correct deficiencies noted while monitoring.

The organization should consider the differences between assumptions and use ("fly as you test"). Assumptions test that all requirements are successfully translated into requirements, verified, and operating as expected. Use tests the behavior of new scenarios, unexpected conditions, or creative functions that the design of the product or service allows. The organization must have documented policies, procedures, and/or processes to record test results for assumptions and use, and mitigation based on benefit versus risk.

Evidence: See General Evidence II.X

Evaluation: See General Evaluation II.X

Appendix

References

NIST Special Publication 800-53 Rev. 5, Security and Privacy Controls for Information Systems and Organizations

NIST Special Publication 800-53A Rev. 5, Assessing Security and Privacy Controls in Information Systems and Organizations