Design Process Standard

V 1.0

Adopted January 3rd, 2023

Standards Committee

Institute of Operational Privacy Design, Inc.
a Florida based not for profit

Introduction

The need for this standard is a culmination of several factors. Though instrumental in socializing the concept of privacy by design, the 7 Foundational Principles developed by the Information and Privacy Commissioner of Ontario in 2009 lack substantive actionable tasks, leaving practitioners unsure how to incorporate the principles into their design processes. Additionally, while several standards around privacy have been promulgated in recent years, the lack of certifiable standards has hampered business-to-business sales, where vendors want to prove to customers their incorporation of privacy into the design of their products and services, and purchasers want assurance of the same. Noticeably absent from Article 25 Data Protection by Design and Default of the General Data Protection Regulation (GDPR) is a mandate on processors or product sellers to incorporate privacy by design. The onus falls on controllers, in GDPR terminology, to ensure data protection is designed in. However, the process or the product developer is often the one who made the design decisions, and the controller is only a passive consumer of the product or service. Finally, this standard came out of a desire to reduce the frequent claims by companies to be doing "privacy by design" without substantive backing for the claim and often without any formality about what privacy by design means to the design process. While this standard will not prevent others from claiming they design for privacy, it at least raises doubt in purchasers as to the validity of those claims when unbacked by a recognized certification.

This standard details the components necessary in a design process to incorporate privacy considerations and reduce privacy risks to individuals. The process could be the design of products, services or business processes and spans the lifecycle from ideation to deployment. While most would consider a design process to be during the ideation, and potentially the development, of a product, service or business process lifecycle, deployment is a necessary phase to consider because once deployed, they almost invariably go through iterations and redesign. In addition, deployment may uncover inaccurate assumptions about context and risk, which require revaluation, redesign and redeployment.

As a final note, this standard covers privacy and is not limited to "data protection" or any specific jurisdictional approach. Privacy is a broader concept than data protection and covers all interactions between individuals and others in society and the social norms governing those interactions. This standard is purposefully ambiguous in that regards. Those wishing to focus on data protection or any subset of human rights and freedom can choose a Risk Model (see Component I.B.), which considers harms to data protection or other rights as the potential concerns. This standard takes a risk-based, as opposed to an absolutist, approach to privacy. With any human activity, there are potentialities, including the potential that privacy expectations and norms are breached. Trading off those risks against benefits to individuals and society (see Component II.C.) and minimizing those risks to individuals and society (see Component II.D.2.) are the goals.

Structural Definitions

Component: A constituent element of this standard. (Note: Components are high-level descriptors of this standard, not a component of a system.)

Phases: The stages of the system lifecycle applicable to this component: ideation, development and deployment. Prerequisite refers to a component that sits outside the system lifecycle

Objective: Goal or desired outcome of the component. The objective describes why the component is important and what it is to achieve.

Description: The detailed explanation of the component.

Implementing Guidance: A description of steps, common pitfalls or clarifying information as to how the organization actually executes the component.

Evidence: Information the organization must present to show it has the component in place.

Evaluation: How the evidence is measured and judged to determine whether it is sufficient to meet the objective and effective at doing so.

Substantive Definitions

Approach: A method, process or procedure to accomplish a goal.

Assessor: An entity who gathers evidence and evaluates whether such evidence shows the organization effectively meets the objective.

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).

Lifecycle: While business activity around a system may be broken down into many lifecycle phases, this standard uses three high-level ones: ideation, development and deployment. The demarcation points between each phase may not necessarily be clean.

- **Ideation** The phase in which the organization is exploring and drawing 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 product, service 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 makes available the system for use. This phase also includes ongoing use and operation of the product, service or business process.

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.

System: The product, service or business process or an element of a product, service or business process.

Residual Risk: A measure of risk remaining after a change in the context, such as applying controls.

Risk: A measure of likelihood and severity of privacy harm using the Risk Factors under a particular risk model.

Risk Model: A representation that elaborates key terms and abstract factors that contribute to or negate privacy harms (see NIST definition).

Risk Factor: An element that 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 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.

Target System: The system being designed, developed or deployed as part of the process. The target system is distinguished from a general system.

Components Outline

The following chart illustrates the major organizational structure of this 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

A. Privacy Governance	B. Risk Model
Evidence and Evaluation	Evidence and Evaluation

Prerequisites are organizational Components that do not relate specifically to the design process. Each prerequisite has its own Evidence and Evaluation requirements.

II. DESIGN PROCESS

Lifecycle: Ideation → Development → Deployment

General Evidence and Evaluation apply to all Design Process Components

A. Identify & Document Target	B. Identify & Document Req.	C. Perform Trade-off Analysis	D. Manage Privacy Risks	E. Verify Context & Requirements	F. Monitor Context
Evidence and Evaluation	Evidence and Evaluation	Evidence and Evaluation	1. Perform Risk Assessment	Evidence and Evaluation	Evidence and Evaluation

a. Contextualize risk factors	E & E
b. Elicit privacy issues	E & E
c. Assess risks	E & E
2. Respond to Risks	
Evidence and Evaluation	

All of the Design Process Components are aligned with one or more of the stages of the product, service or business process lifecycle. The stages are presented at a very high level to avoid conflict with organizations that may have more granular stages.

All Design Process Components have Evidence and Evaluation requirements beyond the general Evidence and Evaluation requirements for the entire design process. The Manage Privacy Risks Component is divided into two subcomponents, the first of which is further subdivided. Each of the subcomponents has Evidence and Evaluation requirements.

I. Prerequisites

Component: I.A. Privacy governance
Phase: Prerequisite
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 its 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, internal communications and audit reports. • 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

I. Prerequisites

I.A. Privacy governance continued

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

- The organization's policies, standards and procedures have been documented, approved, reviewed, communicated and made easily available 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 mandatory training 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 that can be leveraged for risks identified in the risk model.

Component: I.B. Risk model

Phase: Prerequisite

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 (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).

I. Prerequisites

I.B. Risk model continued

Description continued: A privacy risk model or model development process must address: i. Threats ii. Vulnerabilities iii. Adverse consequences iv. Likelihood v. Severity of impact 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 its attention instead 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" Subcomponent stage of the risk assessment. For example, 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.

I. Prerequisites

I.B. Risk model continued

Evidence continued ● 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 whether 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 whether it is consistent with the risk model or whether the process for identifying organizational privacy risk tolerance and appetite will sufficiently match the risk model's quantitative or qualitative measurements.

II. Design Process

General Evidence Requirements for All Lifecycle Components

- The organization must have a documented policy, standard or procedure that addresses the elements of the Component. Such policies, standard or procedures may have exception processes that 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 that addresses the elements in the Description of the Component.

General Evaluation for All Lifecycle Components

The Assessor will examine the evidence and determine whether:

- 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 (i.e., objectivity).
- the minimum 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 whether:

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

II. Design Process

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 about and agreement on 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: ● The purpose/goal/objective of the system ● The intended components of the system ● How the system will 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 ● Wireframe ● User journey
Evidence: See General Evidence
Evaluation: See General Evaluation The Assessor will review the evidence of the target system to determine whether the high-level use case is documented in a way that is useful to those in the organization who are working on the system.

II. Design Process

Component: II.B. Identify and document requirements (functional and nonfunctional)
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 nonfunctional 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. Nonfunctional requirements relate to crosscutting concerns (quality attributes) 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 for ensuring that systems implement nonfunctional requirements that address compliance obligations and organizational privacy values.

II. Design Process

II.B. Identify and document requirements continued

Implementing Guidance continued

- System-specific requirements are those requirements that derive from the objectives of a particular system. A key method of identifying nonfunctional 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 defining system requirements.

Requirements are the what, not the how.

For 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., a double opt-in).

Evidence: Because baseline requirements, although highly advised, are not strictly necessary, evidence of them is mandatory only if the organization claims they are employed (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 they are derived as part of its system lifecycle activities.

II. Design Process

II.B. Identify and document requirements continued

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 select and review a sampling 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 select and review a sampling of system-specific requirements for the Target System selected for review.

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 system owner. 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 lifecycle. Ultimately, however, it is a form of decision analysis.

II. Design Process

II.C. Perform trade-off analysis continued

Implementing Guidance continued

A. Specific methods of performing the analysis should be employed so that it is systematic. Methods employed in systems engineering include but are not limited to:
    1. Pros and 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 that 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 lifecycle processes, including prescribed or suggested methods. Such documentation may have an exception process that allows escalation of decisions outside 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.

II. Design Process

II.C. Perform trade-off analysis continued

Evaluation: The Assessor will review the minimum 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;
- resolve those decisions; and
- document the decisions and justifications.

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

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

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

Subcomponent: 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.

II. Design Process

II.D.1.a. Contextualize risk factors continued

Description continued: 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 its risk assessment process that 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 selects and reviews for contextual factors for target systems (also selected by the Assessor).

Subcomponent: 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 and using its risk model or a system-specific one, identifies and documents the privacy threats, vulnerabilities and consequences that can occur in the target system.

II. Design Process

II.D.1.b. Elicit privacy issues (using the target system documentation and context) continued

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 and documented identified issues in the target system.
Evaluation: The Assessor will determine whether 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.

Subcomponent: 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.

II. Design Process

II.D.1.c. Assess risks continued

Implementing Guidance continued 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.

Subcomponent: 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 its privacy risk tolerance (the former is preferred). 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 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.

II. Design Process

II.D.2. Respond to risk continued

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.

Component: II.E. Verify the target system context and requirements
Phase: Development and Deployment
Objective: To ensure 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.

II. Design Process

II.E. Verify the target system context and requirements continued

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 start uploading photos of relatives, necessitating the need to conduct an assessment of privacy risks for non-customers.
Evidence: See General Evidence
Evaluation: See General Evaluation

Component: II.F. Monitor context
Phase: Deployment
Objective: To ensure post-deployment context does not vitiate the risk assessment and decisions made, requiring reevaluation.
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 ● changes in legislation, policies, directives, regulations, standards and social norms I. Target System: 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 assessing security and privacy controls of the target system to confirm that the controls continue operating effectively. The organization remediates any noncompliant privacy controls or security vulnerabilities.

II. Design Process

II.F. Monitor context continued

Description continued

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 its business strategy, privacy management framework and risk management priorities.
   B. The organization must have procedures for monitoring its merger and acquisition activity or expansion of products and services in 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 eliciting new or changing privacy threats to products and services. The effectiveness of privacy controls against new and revised threats is assessed and appropriate measures are taken to reduce increased risks.
   B. 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 any associated risks.
   C. The organization must have procedures for when the system environment or infrastructure is changed (e.g., on-site versus cloud). Products and services must be reviewed and tested to ensure there is no adverse impact on privacy.
   D. The organization must have procedures for when products, services or processes are outsourced, to evaluate the privacy risks and ensure the privacy controls selected continue to be effective.
   E. The organization must have procedures established for a quick, effective and orderly response to privacy incidents.
   F. 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.

II. Design Process

II.F. Monitor context continued

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, to ensure 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
Evaluation: See General Evaluation