Worksheet 1: Framing Organizational Objectives and Privacy Governance

This worksheet is intended to capture the organizational environment in which the system/product/service is being developed in order to support the development and implementation of appropriate privacy capabilities and increase trust in the organization’s system/product/service. There is no right way to fill out the worksheet as all of the information may not exist. For example, an organization may not have an enterprise risk management strategy or the strategy may not address privacy.

# Task 1: Frame Organizational Objectives

Capturing the mission/business objectives and functional capabilities for the system/product/service help in understanding its purpose in order to determine how to respond to identified privacy risks and support the selection of controls that can mitigate privacy risks while optimizing performance. Identifying how you might highlight or market any privacy protections will help to ensure that your assessment and control selection provide a basis of evidence for these claims and demonstrate the trustworthiness of your system/product/service.

|  |
| --- |
| 1. Describe the mission/business needs that your system/product/service serves. |
|  |

|  |
| --- |
| 2. Describe the functional needs or capabilities of your system/product/service. |
|  |

|  |
| --- |
| 3. Describe any privacy-preserving goals for your system/product/service that you may plan to highlight or market to users or customers. |
|  |

# Task 2: Frame Organizational Privacy Governance

Understand the governance structure for your organization by identifying privacy-related legal obligations and commitments to principles or other organizational policies. This will help you to define the privacy requirements for your system/product/service and better assess the impact of data processing on your organizational priorities, risk tolerances, and values for individuals’ privacy.

|  |
| --- |
| 1. Legal Environment: Identify any privacy-related statutory, regulatory, contractual and/or other frameworks within which the organization must operate. List any specific privacy requirements. |
|  |

| 2. Identify any privacy-related principles or other commitments to which the organization adheres (e.g., Fair Information Practice Principles, Privacy by Design principles, ethics principles). |
| --- |
|  |

|  |
| --- |
| 3. Identify any privacy goals that are explicit or implicit in the organization’s vision and/or mission. |
|  |

|  |
| --- |
| 4. Identify any privacy-related policies or statements within the organization, or business unit. |
|  |

| 5. Document your organization’s risk tolerance with respect to privacy from your organization’s enterprise risk management strategy. |
| --- |
|  |