NATIONAL PRIVACY COMMISSION

*The NPC is an attached agency of the Department of Information and Communications Technology*

# Privacy Impact Assessment

A **Privacy Impact Assessment** (PIA) is a process to evaluate and manage privacy impacts in a PIC or PIP's planned or existing systems technology, programs, process or activities. The process takes into account the nature of the personal data to be protected and evaluates the risks to privacy and security represented by the processing of personal data. The PIA guides the PIC or PIP through the process of understanding the personal data flow in the organization, identifying and assessing various privacy risks, and proposing measures to address these risks. Proposed measures should consider the size of the organization, complexity of its operations, current data privacy best practices and the cost of security implementation.

PIAs should be undertaken for every processing system of an organization involving personal data. It is also important prior to implementation of new programs, projects, processes or measures that have privacy impacts. A change in law or regulation, or changes within the organization may likewise require undertaking a PIA if the changes would affect personal data processing.

It is important to involve the stakeholders of the personal data processing when undergoing a PIA. This may be done by active consultation or by including them as participants in the process. A PIA is an important step in managing risks to privacy and security, strengthening data processing systems, and inspiring trust in the PIC and PIP. It is also a means of demonstrating due diligence for any PIC and PIP.

## Is there a recommended minimum standard for assessing gaps in the control framework?

For agencies that process the personal data records of more than one thousand (1,000) individuals, including agency personnel, the Commission recommends the use of the ISO/IEC 27002 control set as the minimum standard to assess any gaps in the agency's control framework.

## The Contents of the PIA

1. Description of the personal data flow:
    - Categories of personal data held by the agency, including records of its own employees;
    - Source and manner of collection of personal data
    - Persons responsible or accountable for the processing of personal data
    - Purpose of processing, including, where applicable, the legitimate interest pursued by the agency;
    - List of all information repositories holding personal data, including their location;
    - Types of media used for storing the personal data; and
    - Transfers outside the country
    - Organizational, physical and technical security measures in place

2. Assessment of adherence to data privacy principles, including the necessity and proportionality of the processing, the implementation of security measures, and the means for data subjects to exercise their rights

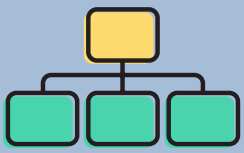
3. Identification and assessment of the risks to the rights and freedoms of data subjects associated with the personal data processing, and any proposed measures to address the risks

## The Control Framework

A control framework is a comprehensive set of measures intended to address the risks identified in the privacy impact assessment. It includes organizational, physical and technical measures that maintain the availability, integrity and confidentiality of personal data and protect the latter against natural dangers such as accidental loss or destruction, and human dangers such as unlawful access, fraudulent misuse, unlawful destruction, alteration and contamination.

It must consider the following:

Nature of the personal data to be protected



Risks represented by the processing, the size of the organization and complexity of its operations

Current data privacy best practices


Cost of security implementation