

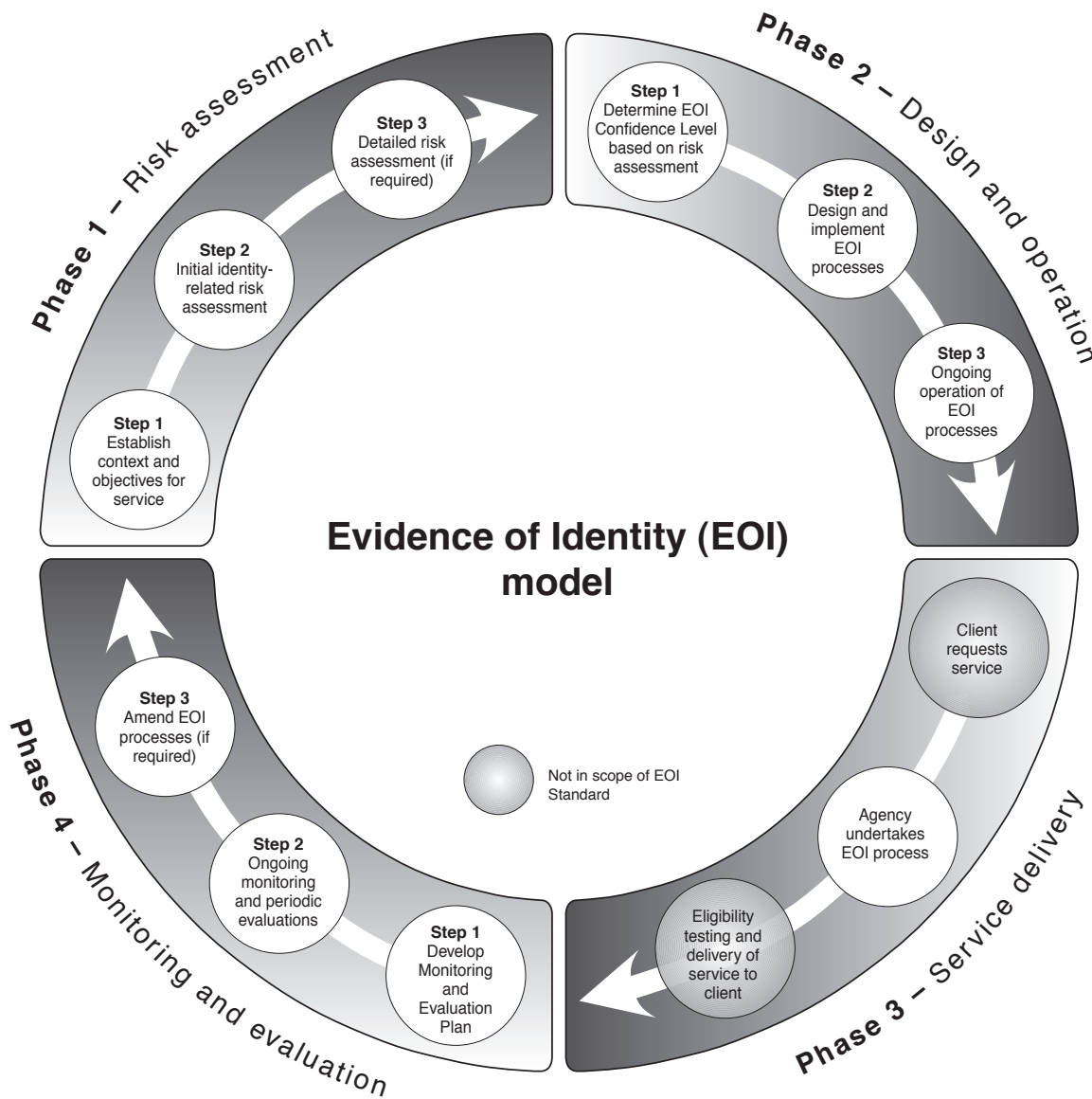
Part 2

Minimum Standard Requirements

2.1 EOI process overview

Figure 1 provides a high-level overview of the process steps that an agency MUST carry out when implementing any EOI processes for services that require an individual’s identity to be established.

Figure 1 – Overview of evidence of identity model



NOTE – Service delivery itself is not within the scope of this Standard. This Standard relates to service delivery only in cases where an EOI process is required before the service can be delivered to an individual.

2.2 Minimum EOI process phases

The main phases of the EOI process shown in Figure 1 are described in Table 2.

Table 2 – Phases of EOI process

Phase	Description
Risk assessment	This phase involves determining the level of identity-related risk within the services that an agency delivers. The results of the identity-related risk assessment will help determine what, if any, EOI process is required for a particular service.
Design and operation	This phase involves designing EOI processes that are appropriate to the level of identity-related risk (identified during the risk assessment phase) in the particular service. Guidance is provided to ensure operationally appropriate EOI processes are implemented.
Service delivery	This relates to the delivery of a service by an agency following confirmation of the individual customer's identity. As such, it is outside of the scope of the standard.
Monitoring and evaluation	This phase involves the ongoing monitoring of EOI processes and periodic evaluation to ensure that each agency's EOI business processes and associated outcomes remain consistent with the EOI process objectives that were established as a result of the risk assessment phase.

2.3 Minimum process step requirements

To achieve the minimum requirements of this Standard, agencies **MUST** ensure that they implement the following process steps. These process steps each form part of one of the process phases listed in Table 2.

Part 3 of this Standard **SHOULD** be followed by agencies to guide implementation of the minimum process step requirements.

2.3.1 Risk Assessment Phase

The agency **MUST** undertake an *identity-related* risk assessment of each of its services. This risk assessment **MUST** involve the following steps:

Step 1 – Establish the context and objectives for the agency's services

When defining the context within which a particular service sits, the agency **MUST** consider, at a minimum, the following factors:

- the business, social, regulatory, cultural, competitive, financial and political environment in which the service exists

- the agency’s key business drivers
- the resources available to the agency (people, systems, processes)
- the impact on stakeholders (both internal and external to the agency).

NOTE – Guidance on how to establish the context and objectives of agency services is provided in 3.3.4.

Step 2 – Carry out an initial risk assessment

The agency MUST determine whether the service results in any of the following:

Financial benefit	Will the individual customer receive a financial payment as a result of the service (e.g. payment of a benefit or grant)?
Non-financial benefit	Will the individual customer receive specific other non-financial benefits as a result of the service (e.g. training)?
Personal information	Will subsequent information about the individual customer be collected and stored by the agency and/or will the service result in the authorised release of personal or sensitive information?
Subsequent use for EOI	Will the service result in the issue of a document or data source that can be used subsequently, by the customer, as a form of EOI?

A positive answer to one or more of the above requires the agency to carry out a formal risk assessment (Step 3).

If the initial risk assessment shows that the service does *not* contain identity-related risk, no further application of this Standard is required.

NOTE – Guidance on carrying out initial risk assessments is provided in 3.3.5.

Step 3 – Carry out a formal risk assessment

The agency MUST identify the consequences that could result from the service being delivered to a person whose identity is incorrectly attributed by the agency. Potential consequences MUST be considered from agency, individual, non-government organisation and general public perspectives.

At a minimum, the agency MUST consider the following risk consequences in relation to the particular service:

- inconvenience, distress, or damage to standing or reputation
- financial loss or liability
- harm to agency programmes or the public interest
- unauthorised release of sensitive information
- personal safety
- downstream effects external to the agency.

Having determined whether any of these consequences apply for the particular service, an evaluation **MUST** be made of the impact level for each consequence.

The agency **MUST** determine the overall level of identity-related risk in the service, based on the evaluation of the above risk consequences and analysis of the likelihood of these consequences occurring. Following this, the agency **MUST** align the service's overall risk rating with one of the following risk categories.

Service risk categories	Description
Nil or negligible	Nil identity-related risk in the service or Negligible level of identity-related risk in the service.
Low	Low level of identity-related risk consequence in the service.
Moderate	Moderate level of identity-related risk consequence in the service.
High	High level of identity-related risk consequence in the service.

Where the service fits within the Nil or negligible risk category, no further application of this Standard is required.

Where the service fits within Low to High risk categories, the agency **MUST** progress to the Design and Operation Phase of the EOI process.

NOTE – Guidance material on how to carry out a formal identity-related risk assessment is provided in 3.3.6.

2.3.2 Design and Operation Phase

Step 1 – Determine required EOI Confidence Level

The agency **MUST** determine the level of confidence required in the identity of the individual, in relation to the level of identity-related risk contained in the particular service.

The risk level assessed for a given service corresponds to the level of confidence required by the agency in establishing the individual's identity.

The different EOI Confidence Levels for services where identity-related risk exists are:

Low Identity Risk Service	—————▶	Low EOI Confidence Level required
Moderate Identity Risk Service	—————▶	Moderate EOI Confidence Level required
High Identity Risk Service	—————▶	High EOI Confidence Level required

Step 2 – Design and implement EOI process

The agency MUST design an EOI process that meets the minimum evidential requirements for the required confidence level identified in Step 1.

NOTE –

- (1) Descriptions of evidential requirements are outlined in Table 8 in Part 3. Guidance on good practice processes to support these evidential requirements is contained in 3.4.7 to 3.4.9.
- (2) Where an agency currently has an EOI process in place for the particular service, the design step MUST be used to identify and close any gaps between current processes and the minimum requirements of this Standard.

Step 3 – Ongoing operation of EOI process

At a minimum, when implementing an EOI process, the agency MUST consider the following operational aspects to ensure that the agency’s ongoing EOI processes meet good practice in each of these areas:

- privacy considerations
- internal controls
- legal considerations
- transition of business processes (if existing processes need to be modified)
- complaints handling
- communication protocols between agencies.

NOTE – Guidance on these considerations is provided in 3.4.16 to 3.4.25.

2.3.3 Monitoring and Evaluation Phase

Step 1 – Develop Monitoring and Evaluation Plan

Prior to the EOI process being implemented, the agency MUST ensure that monitoring and evaluation processes are in place to enable ongoing effectiveness of operational EOI processes.

Step 1.1 – Design monitoring plan

The agency MUST select appropriate performance indicators for monitoring the EOI process, which will form the basis for later evaluation. The agency's choice of performance indicators MUST take the following, at a minimum, into account:

- cost to the agency
- ability to collect the required data/information
- reliability of the performance indicator.

For each performance indicator, the agency MUST determine the method of collection and analysis of data/information and the frequency with which collection and analysis will take place.

Step 1.2 – Design evaluation plan

In carrying out evaluation processes, the agency MUST, at a minimum, document the following:

- rationale for all EOI business processes
- key EOI process objectives to be achieved and the context within which the evaluation is being conducted
- performance indicators used as a basis for the evaluation
- results that the agency considers represent outcomes – successful or otherwise.

Agencies MUST determine the frequency with which evaluation activities will take place. This decision MUST be made prior to any EOI processes becoming operational.

Step 2 – Implement Monitoring and Evaluation Plan

Once the Monitoring and Evaluation Plan and the EOI processes are operational, the monitoring and evaluation processes outlined in the Plan (see Step 1) MUST commence.

Step 3 – Modify EOI processes if required

Where evaluation suggests EOI processes are not adequately meeting objectives, the agency MUST consider modifying the EOI processes. For any modified EOI processes the following, at a minimum, MUST be undertaken:

- testing modified EOI processes before they become operational
- updating the Monitoring and Evaluation Plan to reflect the modified EOI processes.

NOTE – Guidance on monitoring and evaluation of EOI processes is provided in 3.6.