Guideline on Defining Authentication Requirements

1.0. Introduction and Purpose

The purpose of this guideline is to assist departments and agencies [1] in defining their authentication requirements for the delivery of their programs and services in accordance with the Standard on Identity and Credential Assurance and in compliance with the relevant policies and legislation.

This guideline will enable departments to use a standardized approach to defining authentication requirements, while giving them the flexibility to define requirements as they apply to a particular context or to comply with particular constraints.

The Chief Information Officer of the Government of Canada is issuing this guideline to support the Policy on Government Security, the Directive on Identity Management and the Standard on Identity and Credential Assurance.

The relevant requirements set out in the Standard on Identity and Credential Assurance (the Standard) are as follows:

- Identify and evaluate identity and credential risks using an assessment of harms [2] related to a program activity, service or transaction;
- Determine required identity and credential assurance levels using the standardized assurance levels as defined in the Standard; and
- Select identity and credential controls for achieving assurance level requirements using the standardized assurance levels specified in the Standard.

This guideline outlines a simple two-step assessment process. Once departments have completed this process, they should be able to describe the following:

- The assurance level requirements related to a program activity, service or transaction;
- The authentication options as they relate to identity assurance, credential assurance and the authentication process; and
- The residual risks as they relate to identity, credentials and authentication.

Departments should also be able to describe the following:

- Compensating factors;
- Other safeguards; and
- Acceptable risk.

This guideline is intended to be used in conjunction with Communications Security Establishment Canada (CSEC) Information Technology Security Guideline (ITSG-31)—User Authentication Guidance for IT (Information Technology) Systems and with ITSG-33 (IT Security Risk Management: A Lifecycle Approach)—IT (Information Technology) Security Risk Management: A Lifecycle Approach.

This guideline may also be used to assist in defining requirements for financial processing systems in conjunction with the Policy on Internal Control and the Directive on Electronic Authentication and Authorization of Financial Transactions.

1.1 Audience

This guideline is intended for the following users:

- **Program and service delivery managers** who are responsible for identifying and authenticating Government of Canada clients (individuals and business) as part of their program or service delivery requirements. This guideline can be used to assess harms in order to determine standardized assurance level requirements.
- **IT (Information Technology) and security practitioners** who are responsible for recommending, designing, building or providing authentication solutions to meet program requirements. The assessments and assurance level requirements determined by departments may be used in the design and technical recommendation process.

1.2 Application

This guideline applies to systems (both financial and non-financial), services or programs where there is potential harm to users, clients, departments or the Government of Canada as a whole, through inappropriate or unlawful use, whether intentional or unintentional. Potential harm includes loss of privacy, unauthorized disclosure of personal or sensitive information, and unauthorized execution of financial transactions.

This guideline may be used to assist in the analysis of business processes (manual or automated) that include an authentication component. For example, an in-person visit that requires the client to be authenticated before receiving the service.

This guideline may also be used in developing standardized criteria or requirements using the assurance levels. For example, identity assurance requirements, document assurance (integrity) requirements, audit requirements and evidentiary requirements.

This guideline does not recommend specific technologies that should be implemented for the authentication process. For additional information that may be used in conjunction with this guideline, please refer to Related Guidance and Tools.

This guideline does not provide specific guidance on all possible authentication scenarios. Rather, it provides a framework for analyzing authentication requirements and for identifying key decisions for consideration by managers.

This guideline does not apply to authorization or entitlement decisions. Those decisions are usually made independently from the authentication process; departments should consider them separately.

This guideline does not address issues related to the use of electronic signatures, including digital signatures and secure electronic signatures. These issues are addressed in the Personal Information Protection and Electronic Documents Act, the Canada Evidence Act, the Secure Electronic Signature Regulations and related guidance.

1.3 Key Terms and Definitions

The following are some of the terms used in this guideline, as defined in the Standard. For a complete list of terms and definitions, please refer to the Standard.

Assurance
A measure of certainty that a statement or fact is true.

Assurance level
A level of confidence that may be relied on by others. [3]

Authentication
The process of establishing truth or genuineness to generate an assurance. [4]

Authoritative party
A federation member that provides assurances (of credential or identity) to other members (relying parties).

Authoritative source
A collection or registry of records maintained by an authority that meets established criteria.

Credential
A unique physical or electronic object (or identifier) issued to, or associated with, an individual [*], organization or device.

Credential assurance
The assurance that an individual [*], organization or device has maintained control over what has been entrusted to him or her (e.g., key, token, document, identifier) and that the credential has not been compromised (e.g., tampered with, corrupted, modified).

Credential assurance level
The level of confidence that an individual [*], organization or device has maintained control over what has been entrusted to him or her (e.g., key, token, document, identifier) and that the credential has not been compromised (e.g., tampered with, corrupted, modified).

Federation
A cooperative agreement between autonomous entities that have agreed to work together. The federation is supported by trust relationships and standards to support interoperability.

Identity
A reference or designation used to distinguish a unique and particular individual [*], organization or device.

Identity assurance
A measure of certainty that an individual [*], organization or device is who or what it claims to be.

Identity assurance level

The level of confidence that an individual [*], organization or device is who or what it claims to be.

Identity management
The set of principles, practices, processes and procedures used to realize an organization's mandate and its objectives related to identity.

Identity risk
The risk that an individual [*], organization or device is not who or what it claims to be.

Relying party
A federation member that relies on assurances (of credential or identity) from other members (authoritative parties).

2.0. Context

2.1 Government of Canada Cyber-Authentication and Federating Identity

Authentication is "the process of establishing truth or genuineness to generate an assurance." This definition is generic and reflects the fact that authentication is a broad concept that can cover many aspects. In most cases, authentication requirements and the associated processes are defined in the context of a program requirement or a technology solution. Although these definitions and requirements are appropriate in their specific contexts, it may be difficult to apply them horizontally across many different contexts, so the use of a standardized service or component may be more appropriate.

In 2008, the Government of Canada launched the Cyber-Authentication Renewal Initiative to articulate a vision and develop a strategy to move toward a standards-based federated architecture that would allow for the use of other credentials external to government.

In 2009, Federating Identity Management in the Government of Canada: A Backgrounder was finalized. This document describes the federal government's vision of federating identity management to develop next-generation online authentication services. This vision, in conjunction with the Treasury Board of Canada Secretariat's Directive on Identity Management, provides the direction for developing additional policy instruments and implementing technological solutions.

2.2 Alignment with the Pan-Canadian Assurance Model

This guideline is intended to put into practice the concepts described in the Pan-Canadian Assurance Model, a generalized assurance model that can be used to help different jurisdictions develop and agree on standards to achieve interoperability.

At its completion in early 2010, the Pan-Canadian Assurance Model represented a common understanding across federal, provincial, territorial and municipal jurisdictions of the key terms, definitions and concepts that could be applied in conjunction with existing standards or to develop new standards. The Pan-Canadian Assurance Model was a primary resource in developing the Standard on Identity and Credential Assurance and this guideline.

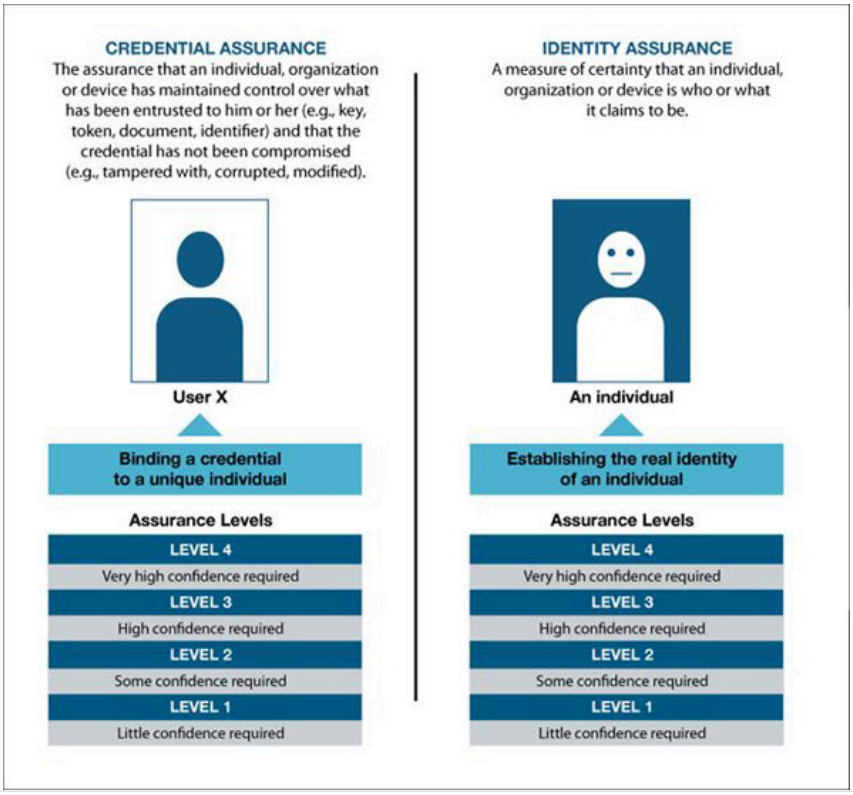
Departments should familiarize themselves with the Pan-Canadian Assurance Model.

2.3 Separation of Credential and Identity

A key element of the Cyber-Authentication Renewal Initiative has been the separation of identity from credential. This separation has enabled the first phase of implementation of next-generation services to support the federation of credentials. The next major phase that the Government of Canada is undertaking is federation of identity.

The Standard, consistent with the Pan-Canadian Assurance Model, makes a distinction between "credential assurance" and "identity assurance". Figure 1 illustrates this distinction.

Figure 1: Credential Assurance vs. Identity Assurance



▶ Figure 1 - Text version

Credential assurance relates to the process of binding a credential to a unique individual. This binding process does not necessarily involve the identity of the individual. When a credential is authenticated, the process provides a credential assurance that ensures that it is the same individual who previously received the credential.

Identity assurance relates to the process of establishing the real identity of an individual. When an identity is authenticated, the process ensures that the individual is who he or she claims to be.

Credential and identity assurance processes may be implemented using controls of increasing strength that correspond to the increasing assurance levels.

In practice, most processes related to providing and using credential and identity assurances have been combined. However, the Government of Canada, in its Cyber-Authentication Renewal Initiative has separated these processes to facilitate a phased approach to federation.

This separation between identity and credential becomes crucial when departments have to integrate into a federation in a way that complies with privacy and program legislation requirements. The separation allows for the "trusting of credentials," which means that a department can have confidence that a credential issued to an individual by another department or organization is being used by the individual to whom it was issued even though it may not know the identity of the individual. The assurance of the individual's identity is the responsibility of the department that issues the credential.

From the perspective of the individual, this separation also has important privacy and choice implications. It also allows an individual to use credentials anonymously or pseudonymously, to use the same credential across different services, or to use different credentials across different services.

More detailed information on the separation of identity and credential can be found in the Pan-Canadian Assurance Model and in Federating Identity Management for the Government of Canada: A Backgrounder.

2.4 Assurance Levels and Trust Frameworks

The assurance levels defined in the Standard on Identity and Credential Assurance and used in this guideline are consistent with emerging industry and public sector trust frameworks (e.g., Kantara Initiative, Open Identity Exchange, eID Interoperability). A trust framework defines the set of policy, business and technical requirements that members of a federation have agreed to comply with. Central to these frameworks is the recognition that assurance is a critical ingredient in formalizing federated arrangements and a necessary component of collectively managing risk across a federation.

In its most generic sense, an assurance level conveys a degree of confidence required or a level of trust between two or more parties where one party has agreed to rely on another party to carry out activities or processes on its behalf.

A federation is a multilateral agreement between parties, where selected federation members, in the role of authoritative parties, are trusted to provide assurances. Other federation members, in the role of relying parties, rely on or trust these assurances.

The benefit of articulating a generic, standardized and required assurance level (known as an assurance level requirement) is that it supports federation (and multilateral agreements) and facilitates the selection and implementation of standardized requirements and solutions that are required by the emerging trust frameworks.

The Standard on Identity and Credential Assurance formalizes the key concepts required for identity federation. The central concept is assurance level. The assurance level is expressed as a standardized generic level from 1 to 4. Table 1 describes the framework for assessing identity and credential assurance levels, as defined in the Standard.

Table 1: Assurance Level Framework

Level	Identity Assurance	Credential Assurance

Level	Identity Assurance	Credential Assurance
4	**Very high confidence required that an individual is who he or she claims to be.** Compromise could reasonably be expected to cause serious to catastrophic harm.	**Very high confidence required that an individual has maintained control over a credential that has been entrusted to him or her and that that credential has not been compromised.** Compromise could reasonably be expected to cause serious to catastrophic harm.
3	**High confidence required that an individual is who he or she claims to be.** Compromise could reasonably be expected to cause moderate to serious harm.	**High confidence required that an individual has maintained control over a credential that has been entrusted to him or her and that that credential has not been compromised.** Compromise could reasonably be expected to cause moderate to serious harm.
2	**Some confidence required that an individual is who he or she claims to be.** Compromise could reasonably be expected to cause minimal to moderate harm.	**Some confidence required that an individual has maintained control over a credential that has been entrusted to him or her and that that credential has not been compromised.** Compromise could reasonably be expected to cause minimal to moderate harm.
1	**Little confidence required that an individual is who he or she claims to be.** Compromise could reasonably be expected to cause minimal to no harm.	**Little confidence required that an individual has maintained control over a credential that has been entrusted to him or her and that that credential has not been compromised.** Compromise could reasonably be expected to cause minimal to no harm.

Once an assurance level requirement is determined, it can be used to determine authentication options for identity assurance and credential assurance and to determine the authentication process. The assurance level requirement is also useful when there is a need to federate with (i.e., trust) other parties. Depending on the scope and nature of the federation, these requirements may refer to trusting credentials (credential federation) or to trusting identity (identity federation).

2.5 Adoption of Standards-Based Services

A key principle under the Government of Canada Cyber-Authentication Renewal Initiative is to enable departments to adopt standards-based services that are commercially available or to use standardized industry frameworks where possible. The first phase of Cyber-Authentication Renewal has been the federation of credentials, which has resulted in authentication service components that departments must adopt (see Section 3.6, Mandatory Use of Cyber-Authentication Services).

The next major phase of Cyber-Authentication Renewal is the federation of identity. This phase will be significantly more complex, and standardized components and commercial services are only beginning to become available. Departments should become familiar with the emerging frameworks so that when new components and services are available they will be ready to adopt them or to align their practices with them.

This guideline is intended to assist departments in their alignment or adoption process by providing a standardized framework for assessing assurance (the four-level scale) and to encourage them to use the emerging trust frameworks, standards, technologies or commercial services as they become available.

The Government of Canada is actively involved in developing federation frameworks and related standards. Departments may obtain more detailed information from the Cyber-Authentication Renewal team.

The Government of Canada is committed to providing Canadians with secure access to online information and services. The first generation of online authentication services was based on proprietary technologies. Over time, these services are being replaced by standards-based services.

By December 2012, the Government of Canada will have acquired and implemented two standards-based cyber-authentication services for mandatory use by departments:

1. **GCKey**, a managed credential authentication service provided by contract to the Government of Canada; and
2. **Credential Broker Service (CBS)**, a commercial service provided by contract to the Government the Canada. The CBS (Credential Broker Service) will enable users to use external credentials that they already have with financial institutions.

As part of the Cyber-Authentication Renewal Initiative, the Canada Revenue Agency also provides its own credential management solution for individuals, businesses and representatives to use when accessing its online services.

2.6 Related Risk Management Methodologies

In August 2010, Treasury Board of Canada Secretariat released the Framework for the Management of Risk. This framework recognizes that failure to effectively manage risks can result in increased program costs and missed opportunities, which can compromise program outcomes, and ultimately public trust. With the recent emergence of trust frameworks, there is increasing awareness that, in addition to managing risks, formalizing trust relationships with other organizations (i.e., federating), is a means of reducing program costs and streamlining processes. In other words, the combination of reducing risk and increasing trust can increase both effectiveness and efficiency.

A risk assessment asks two questions: “What is the injury level?” and “What is the likelihood of that injury occurring?” The goal of a risk assessment is to better understand the risk in order manage it. A risk level is generally characterized as the product of injury level (low, medium or high) and the likelihood of occurrence (low, medium or high). The resulting risk level is managed in various ways, including acceptance, avoidance, reduction or sharing.

An assurance level assessment asks one question: “What is the minimum level of confidence required to achieve a business or program objective?” The goal of an assurance level assessment is to understand the degree of confidence (assurance level) that one party can rely on another party to provide.

An assurance level assessment and a risk assessment are similar in that both centre on assessing harms. However, an assurance level assessment does not use the concept of likelihood.

An assurance level assessment takes a “What if?” approach that compels the assessor to evaluate the potential harms regardless of the likelihood of them occurring. In other words, it is assumed that the occurrence will happen. This approach means that situations can arise where a service is considered low-risk because of a very low likelihood of a harm occurring but still requires a higher level of assurance because of the nature of the transaction or the information being accessed (e.g., personal information).

An assurance level assessment is intended to complement a conventional risk assessment by formalizing the level of assurance required between two parties (i.e., members of a federation).

2.7 Related IT Security and Privacy Assessment Frameworks

IT (Information Technology) security and privacy assessment models also incorporate risk management concepts.

IT (Information Technology) security risk assessment models focus on the potential loss of confidentiality, integrity or availability in relation to the protection of sensitive and valuable assets. These models characterize the vulnerabilities and the sensitivity of organizational assets, as well as the threats to them and the associated injury levels, to arrive at an assessment of the risks and a recommendation on the security controls that should be implemented. Security models also encompass the concept of robustness—the combination of the strength of the control and the assurance that it is implemented correctly.

Privacy impact assessment models focus on the potential loss of privacy in relation to the protection of individuals’ personal information. These models characterize the nature and sensitivity of personal information and of activities related to the collection, use and disclosure of this information.

Currently, there is no broad consensus on how the emerging trust (i.e., assurance level) frameworks, security and privacy assessment frameworks should map to each other. Their practitioners should therefore apply them in a collaborative fashion in order to provide departments with the best information possible on which to base decisions.

2.8 Application to the Integrity of Financial Transactions

This guideline may be applied to systems involving financial transactions. These systems are subject to the Policy on Internal Control, which is issued by the Office of the Comptroller General (OCG) and supported by the revised Directive on Electronic Authentication and Authorization of Financial Transactions.

This revised directive supersedes the previous policy and the requirement that a digital signature be used to authorize electronic business transactions. The new directive states that Chief Financial Officers are responsible for:

Obtaining an appropriate level of assurance that risks to the integrity of financial transactions have been properly assessed and that appropriate key controls to mitigate these risks are documented, in place as designed, and operating effectively in an ongoing manner.

This new requirement is intended to give departments more flexibility in developing authentication solutions within the context of financial systems. Departments may therefore use this guideline in determining the most appropriate authentication solutions for financial systems. Departments should contact the OCG (Office of the Comptroller General) for detailed advice on applying this guideline.

3.0. Assurance Level Assessment Process

3.1 Overview of Assessment Process

The assurance level assessment process helps departments determine the assurance level requirement for credentials and identity and determine authentication solutions for programs, services and transactions.

The assurance level assessment process has two steps:

Step 1: Determine the assurance level requirement

This step answers the following question from the department's perspective: "What is the minimum assurance level we need to achieve the program objectives, deliver the service or properly execute the transaction?"

This step is carried out by the responsible manager, who knows the clientele, the nature of the program or service, and the strategic outcomes that are to be achieved.

Step 2: Determine the authentication requirements

This step answers the following question from the department's perspective: "What methods, safeguards or measures do we have already, or do we need to put in place or rely on?"

This step provides a framework for the department and the various IT (Information Technology) and security practitioners to work together on key decisions required for determining authentication requirements. These decisions are expressed in terms of the standardized levels.

3.2 Step 1: Determine Assurance Level Requirement

The purpose of Step 1 is to determine the minimum assurance level needed to achieve program objectives, deliver a service or properly execute a transaction. This minimum assurance level is referred to as the "assurance level requirement."

A standardized assurance level requirement indicates the overall level of confidence required to carry out a program activity, service or transaction. Departments may use the assurance level requirement, in conjunction with standardized frameworks, to determine the appropriate controls or safeguards

that should be implemented in their organization. Departments may use the assurance level requirement to determine what they require as a relying party or as an authoritative party.

As indicated earlier, determining the assurance level requirement can involve the same inputs used in risk assessments. However, the assessment of the assurance level takes a “What if?” approach, which yields a level of confidence rather than a level of risk. In this approach, assessors are advised to consider the harms that would occur as a result of a compromise, no matter how remote the likelihood of occurrence.

The assessment is based on the nature and type of the program and activities. By breaking down the possible harms into different harm categories, the worksheet helps assessors identify and understand the risks across these different categories.

Step 1 is carried out using the worksheet found in Appendix A. The worksheet helps departments assess the potential harms and thereby determine an assurance level requirement.

The **Assurance Level Requirement Worksheet** uses the following harm categories:

1. **Inconvenience, distress, loss of standing or reputation:** Relates to harms including delay, embarrassment, loss of confidence, or damage to reputation.
2. **Financial loss:** Relates to harms involving financial loss. Specific dollar amounts depend on the party that is being impacted.
3. **Harm to program or to public interest:** Relates to harms including failure to achieve expected outcomes, loss of public trust, or decrease in the economic or social well-being of Canadians.
4. **Unauthorized release of sensitive personal or commercial information:** Relates to harms involving the unauthorized disclosure of personal or commercial information.
5. **Unauthorized release of sensitive government information:** Relates to harms involving the unauthorized disclosure of classified information, protected information or confidences of the Queen’s Privy Council (i.e., Cabinet confidences).
6. **Civil or criminal violations:** Relates to harms involving intentional or unintentional facilitation of a civil or criminal violation.
7. **Personal health or safety:** Relates to harms involving physical or psychological injury to an individual.
8. **National interest:** Relates to harms affecting the national interest.

Guidelines for Completing Step 1

- The assessment should be performed by the responsible manager. This person should have a detailed knowledge of the program, service or transaction. The assessment draws on this knowledge and is based on business or program-related factors, including the following:
    - The program objectives, including higher-level strategic objectives or strategic outcomes that program activities are intended to achieve. Consideration of harms could include the consequences of not achieving these objectives or outcomes.

- The nature and type of program, service or transaction that is being assessed. Consideration could include the consequences of harms to program owners and managers responsible for carrying out program activities, services or transactions.
- The clients, stakeholders and other interested parties that may be affected by harms.
- Intangible or global factors that may be relevant, such as the public interest or national security.

- The assurance level assessment should be conducted **without** regard to delivery channels or to existing system safeguards or business processes. The assessment is based strictly on the nature of the program, service or transaction and on its clients or stakeholders.
- The assurance level requirement is determined independently from the categorization of information as protected or classified, for example.
- When conducting the assessment, the responsible manager should define the business context and focus the assessment on this context. The business context could include the following:
    - Whether the program, service or transaction is externally facing (e.g., client-focused) or internally facing (e.g., employee-focused);
    - The type and nature of clients affected by the program, service or transaction (individuals, professionals, or businesses); and
    - Legislative and jurisdictional considerations.
- Departments may decide that certain harm categories do not apply to their assessment process. If this is the case, they should provide a rationale for that decision.
- The assessment should consider only the harms that can be directly attributed to the specific program activity, service or transaction being assessed. In other words, it should focus on the harms that could stem directly and immediately from the failure of a program activity, service or transaction in cases where it is the sole contributing factor.
    - **Example:** An individual applying for an official travel document (e.g., a passport) provides false or misleading information.

  The act of providing false or misleading information is grounds for criminal prosecution and can be directly attributed to the applicant. This harm would be considered a direct harm and should be considered in the assurance level assessment.
- Conversely, the assessment should **not** take into account indirect (or ensuing) harms that might occur where the failure of a program activity, service or transaction that may be one of several contributing factors to a subsequent (and possibly greater) harm over which the department has little or no control. [6]
    - **Example:** A fraudster gains access to personal information that is made available publicly through a user's social media profile. The fraudster then uses

this information to commit credit card fraud.

The act of gaining access to publicly available personal information may not be considered grounds for criminal prosecution; however, its subsequent use by a fraudster may be. With respect to the social media service, the potential for credit card fraud is an indirect harm and should not be considered in the assurance level assessment.

- Departments may have separately defined their services on the basis of a specific delivery channel or implementation mechanism. From a business standpoint, however, these channel-specific services are usually a subset of a more generic program, service or transaction and therefore can be addressed with a single assessment. When assessing channel-specific services, assessors should first identify the business service, and it is this business service (regardless of the delivery channel) that should be the target of the assessment.
- Departments are free to decide how granular they want their assessments to be. Separate assessments may be conducted at a program level, at a service or service cluster level, or at a transaction level. The more granular the assessment, the greater the effort required.
- Departments should perform the Step 1 assessment at the business transaction level to ensure that they properly consider all potential harms within a service or program.
- Departments should decide whether the assessment is an informal process or a formal process that is signed off by the responsible manager.
- Departments should be prepared to provide evidence that the assessment process has been carried out.
- The assurance levels may be extended to serve as a general scheme to link related business or program requirements and technical specifications that employ an assurance level framework. This is useful when integrating other standards-based frameworks involving credentials, identities, authentication, etc.
- When completed, the assurance level requirement must be expressed as a standardized, discrete **Level 1** through **Level 4**. It may not be expressed as a variant (e.g., “Level 2+”).
- The Step 1 assessment should be carried out periodically (e.g., annually) or whenever there is a fundamental change concerning one or more of the following:
    - The nature of the program, service or transaction;
    - The nature of the information being used;
    - The context or clientele (e.g., a new client demographic will be using the service); and
    - Systemic matters (e.g., departmental reorganization, new system architectures, changes in legislation).

3.3 Step 2: Determine Authentication Options

The purpose of Step 2 is to determine the authentication options that will be used to achieve the assurance level requirement determined in Step 1.

Before determining the authentication options, a department should consider many factors, such as the use of mandatory services, technical requirements, cost, privacy and security requirements, and user acceptability.

In many cases, departments may be unable to, or may not want to, implement their own authentication solution. Instead, they may decide to have other organizations (i.e., providers) carry out the entire solution or selected components of it on their behalf. Providers may be external entities or commercial entities operating under a contract or under another arrangement, such as federation.

In certain cases, the decision to contract out or to federate certain components of an authentication solution has already been made. For example, the Government of Canada has already decided to federate credentials through the use of commercial services (see Section 3.6, Mandatory Use of Cyber-Authentication Services). Also, departments are required to use certain standardized components and services.

Departments should analyze their authentication options and develop recommendations for the three requirement areas:

- **Identity assurance requirements:** The minimum requirements to establish the identity of an individual to a given level of assurance (Level 1 through Level 4). These requirements are set out in Appendix C of the Standard on Identity and Credential Assurance. For more details on identity assurance requirements, refer to the Guideline on Identity Assurance (to be published in 2013).
- **Credential assurance requirements:** The minimum requirements to ensure that an individual has maintained control over a credential that has been issued to him or her and that the credential has not been compromised. These requirements are set out in the related guidance, ITSG (Information Technology Security Guideline - User Authentication Guidance for IT Systems)-31, published by CSEC (Communications Security Establishment Canada).
- **Authentication requirements:** The minimum technical design and/or business process requirements that are necessary to carry out an authentication process (electronic or manual). The requirements for electronic authentication are set out in the related guidance, ITSG (Information Technology Security Guideline - User Authentication Guidance for IT Systems)-31 and ITSG-33 (Information Technology Security Guideline - User Authentication Guidance for IT Systems), published by CSEC (Communications Security Establishment Canada).

  For manual channels (e.g., in-person, telephone and correspondence/mail), “standardized” requirements should be aligned with departmental or industry best practices. At present, there are few standards or guidelines related to these other channels.

Guidelines for Completing Step 2

The assurance level requirement determined in Step 1 is the **minimum** assurance level that an overall authentication solution should achieve. An **ideal** authentication solution would meet the minimum requirement in all three areas: identity, credentials and authentication.

For example, an ideal Level 3 authentication solution would implement standardized Level 3 requirements for identity assurance, credential assurance and authentication.

However, it may not be feasible or cost-effective for a department to implement an authentication solution using the standardized requirements specified for the assurance level requirement determined in Step 1. If that is the case, the department may consider implementing standardized requirements for a lower assurance leveland mitigate the residual risk through alternative methods such as compensating factors or other safeguards (see Section 3.4, Mitigation of Residual Risks). The department might also consider accepting the residual risks (see Section 3.5, Risk Acceptance).

The residual risks that departments should consider correspond to the three requirement areas:

- **Identity risk:** The risk that an individual, organization or device is not who or what it claims to be. Examples of identity risk include individuals fraudulently registering for a service, using false or forged documents, and impersonating another or a fictional person.
- **Credential risk:** The risk that an individual has lost control over the credential that has been entrusted to him or her (i.e., that, without their knowledge or consent, it is being used by another individual). Examples of credential risk are individuals fraudulently using lost or stolen passwords, tokens or devices.
- **Authentication risk:** The risk that the authentication process has been compromised. This risk relates closely to the overall security of a system or process (electronic or manual). Examples of authentication risk in an electronic environment are “man-in-the-middle” attacks and key logging. Examples of authentication risk in a manual environment include risks that result from counterfeiting, human error or malfeasance.

These three risk areas are not discrete (e.g., increased credential risk can lead to increased identity risk and vice versa). By analyzing the risks separately, however, departments can gain further insight into vulnerabilities and threats.

For each requirement area (identity, credential and authentication), departments should refer to Table 2 for guidance when they decide to use the following authentication options:

a. **Implementing within the department:** This is the situation when a department decides not be a relying party or a member of a federation. It also may be the situation when a department is the authoritative party and is therefore responsible for implementing the requirements.
b. **Relying on another party:** This is the situation when a department decides to rely on another party to implement requirements on its behalf. This may be achieved in the following ways:
    i. Formal or informal bilateral or multilateral agreements (e.g., memorandums of understanding);
    ii. Contracts with commercial service providers; or

iii. Participation in a federation.

Table 2 outlines what departments should do when a selected authentication option is **equal to** the assurance level requirement determined in Step 1 and when the selected option is **lower than** the assurance level requirement determined in Step 1.

Table 2: Considerations for Authentication Options

Authentication Option	Implementation Option	
	Within the Department	**Rely On Another Party**
i. **Equal to** assurance level requirement	• Ensure that department complies with requirements for assurance level requirement determined in Step 1	• Ensure that provider complies with requirements for assurance level requirement determined in Step 1 If participant in **federation**: • Ensure that member (or service provider) meets criteria established by federation to provide assurance level [7] determined in Step 1

Authentication Option	Implementation Option	
	Within the Department	**Rely On Another Party**

ii. **Lower than** assurance level requirement	• Provide rationale for selecting implementation using lower assurance level (e.g., cost, usability, mandatory service, technical feasibility)
	• Describe potential threats and vulnerabilities that might be exploited, including breaches
	• Describe risk mitigation measures for identity, credential and/or authentication risk
	• Include descriptions of the following:
	  ◦ Compensating factors
	  ◦ Other safeguards
	  ◦ Acceptance of risk
	• Ensure that department complies with requirements for lower assurance level requirement determined in Step 1
		• Provide rationale for selecting provider at lower assurance level (e.g., cost, usability, mandatory service, technical feasibility)
		• Describe potential threats and vulnerabilities that might be exploited, including breaches with the department or the provider
		• Describe risk mitigation measures, including terms and conditions in specified in contracts or agreements with provider or federation members
		• Include descriptions of:
		  ◦ Compensating factors
		  ◦ Other safeguards
		  ◦ Acceptance of risk
		If participant in **federation**:
		• Ensure that member (or service provider) meets criteria established by federation to provide assurance level as determined in Step 1
		• Ensure that department understands its responsibilities for managing residual risk

3.4 Mitigation of Residual Risks

The Framework for the Management of Risk defines residual risk as “the remaining level of risk after taking into consideration risk mitigation measures and controls in place.”

For each requirement area (identity risk, credential risk and authentication risk), departments should be able to describe how residual risks are being mitigated or why they are being accepted.

- **Compensating factors:** [8] Additional measures used during the authentication process to reduce a risk. A compensating factor may be used when part of the authentication process does not meet an assurance level requirement. A compensating factor is intended to mitigate the residual risks or to counter new (anticipated or unanticipated) threat possibilities. The use of compensating factors mitigates residual risk; it does not raise the assurance level.
- **Other safeguards:** Additional measures used in addition to the authentication process to reduce risk. Other safeguards may be security control mechanisms used downstream or "flags" that are raised to initiate exceptions or interventions.

Guidelines for Compensating Factors

Compensating factors **should**:

- Be appropriate to the program, service or transaction context; and
- Be dynamic and easily adaptive, particularly in a highly fluid threat environment (e.g., a public-facing Internet service).

Compensating factors **should not**:

- Place an unnecessary burden on the client being authenticated (otherwise, the client might abandon the service).
- Use personal or program-specific information that might raise privacy concerns. If such information is used, its use should be strictly limited to a specific program, service or transaction. The use of this information may result in unforeseen vulnerabilities or open a new threat vector and thereby be counterproductive.
- Be used to escalate the assurance level of a credential for use elsewhere (e.g., enable a Level 2 credential to be relied on as a Level 3 credential).

Examples of compensating factors include the following:

- Shared secrets;
- Identity validation (validating identity information collected as part of an identity assurance process);
- Program validation (validating program information collected as part of a program or service administrative process);
- Token/grid card challenge;
- Reverse Turing test (to determine whether a user is human); and
- Out-of-band confirmation.

The principal benefit of a compensating factor is that it allows for flexibility in the design of an authentication solution. This flexibility is required if the authentication process is subject to business or usability constraints or if the authentication process has to adapt to a changing threat environment (i.e., new threat agents or new vulnerabilities).

Compensating factors also have drawbacks. Because they are customized, they increase overall costs and process complexity. Increased complexity can lead to a more frustrating user experience and to additional maintenance. So, while attractive in the short run, compensating factors can be problematic in the long run. The factors used may become ineffective as threat agents adapt, or they may introduce privacy risks and impose additional security constraints if the factors use program-specific or personal information. If compensating factors are to be considered in an authentication solution, the benefits and drawbacks should be carefully weighed against one another.

Electronic authentication technologies are evolving quickly due to rapidly changing technology and the constantly changing cyber-threat landscape. Departments should be aware of the latest best practices and standards that are being developed to address these threats.

Guidelines for Other Safeguards

The authentication process may exist within a larger context of security control mechanisms that mitigate risks. Although a transaction may require a higher assurance level, the additional risk may be mitigated by other security controls that are not related to authentication but that are within the system or are downstream from the authentication process.

Other safeguards should be designed to capture and contain the downstream effects of an authentication error. For example, if an authentication error results in unauthorized access, the resulting access should be compartmentalized to a subset of low-risk transactions or non-sensitive information.

3.5 Risk Acceptance

For the purposes of this guidance, the level of residual risk depends on the compensating factors and on other safeguards that work in conjunction with the authentication process.

Guidelines for Risk Acceptance

The responsible manager should be well informed in order to decide whether the level of residual risk is acceptable for the department and to ensure that the potential consequences are managed accordingly.

Risk acceptance should be:

- Documented and signed off by the appropriate risk management authority, i.e., the level of management authority required for sign-off should be commensurate with the assurance level or the relative magnitude of the risk being accepted (e.g., Level 4 might require sign-off by the deputy head);
- Appropriately shared among participating parties with respect to potential liabilities and consequences; and
- Clearly communicated to all parties involved, including clients.

Departments should also be prepared to describe how the consequences will be managed on behalf of clients who may realize the potential harms.

3.6 Mandatory Use of Cyber-Authentication Services

The mandatory use of cyber-authentication services enables departments to achieve cost savings and technical efficiencies by ensuring that the Government of Canada builds or buys only once and then leverages commercial infrastructure for common use. It also enables the government to optimize and consolidate service delivery channels in support of secure e-services and to maintain the confidentiality and privacy of client information in a consistent manner.

The mandatory use of cyber-authentication services is subject to the Treasury Board of Canada Secretariat Common Services Policy and the subsequent 2006 Treasury Board decision on secure channel mandatory services. In relation to this guideline, two cyber-authentication services are considered mandatory: external credential management and internal credential management.

- **External Credential Management (ECM) Service:** A credential management service for external users (individuals or businesses). The previous implementation of ECM known as ePass has been replaced by the following services:
    - **Credential Broker Service (CBS):** A commercial service provided by contract to the Government of Canada that enables users to use external credentials they already have with financial institutions to securely authenticate in order to access government services.
    - **GCKey:** A Government of Canada branded credential for use by clients who do not have, or who choose not to use, a credential with a financial institution.
- **Internal Credential Management (ICM) Service:** A credential management service that provides government with a standard set of registration processes for issuing a unique digital credential that enables access to internal online services. This service is composed of a set of services supporting the registration and authentication of employees. The current implementation of ICM has one component:
    - **myKEY:** An identity-based credential intended for full-time Government of Canada employees. myKey was formerly known as PKI (Public Key Infrastructure) Key, ID-based Certificate, Entrust Profile or PKI (Public Key Infrastructure) Certificate. myKey is used to access applications such as compensation Web applications and to access personnel information such as payroll.

As part of the Cyber-Authentication Renewal Initiative, the Canada Revenue Agency also provides its own credential management solution for individuals, businesses and representatives to access the Agency’s login services.

Policy Exemptions and Treasury Board Approval

In exceptional circumstances, neither ECM nor ICM is an appropriate authentication solution. In such cases, a policy exemption is required. An exemption request is typically part of a Treasury Board submission and approval process. In seeking exemptions, departments must satisfy the relevant

Treasury Board policy centres that the exemption request is valid and must submit a business case as part of a Treasury Board submission that presents the anticipated advantages of granting an exemption.

3.7 Federation

Federation refers to arrangements that enable parties to provide and to rely on assurances. Federation involves authoritative parties that provide assurances and relying parties that use these assurances to support their business processes or program activities. Federation is achieved through arrangements that are built on a common framework supported by standards, formalized agreements and established criteria.

The Treasury Board of Canada Secretariat is currently undertaking initiatives on federating identity. Departments should contact the Cyber-Authentication Renewal Initiative for further information.

4.0. Related Guidance and Tools

This section provides an overview of guidelines that should be used in conjunction with this guideline.

4.1 Guideline on Identity Assurance

The Guideline on Identity Assurance is a companion guideline. It provides guidance on the implementation of requirements specified in Appendix C of the Standard on Identity and Credential Assurance.

4.2 Privacy Impact Assessments

The Treasury Board of Canada Secretariat Directive on Privacy Impact Assessment requires that departments carry out a privacy impact assessment for new or substantially modified programs or activities that involve the creation, collection and handling of personal information.

Appendix C of the Directive prescribes a standardized identification and categorization of privacy risk areas that must be included in each privacy impact assessment. The categories are as follows:

- Type of program or activity;
- Type of personal information involved and context;
- Program or activity partners and private sector involvement;
- Duration of the program or activity;
- Program population;
- Technology and privacy; and
- Personal information transmission.

The privacy impact assessment must also include an evaluation of the level of potential risk, on a scale of 1 (lowest) to 4 (highest).

Although these risk categories may be considered roughly analogous to the assurance levels set out in this guideline, the privacy impact assessment should be conducted independently from the assurance level assessment. At present, there is no specific linkage between the two assessments;

however, departments can compare the results of the assessments to ensure that they contribute to a more complete and consistent understanding of the overall risks involved.

4.3 Threat and Risk Assessments

Departments may want to conduct more generalized security risk assessments using the Harmonized Threat and Risk Assessment (TRA) Methodology, which is jointly published by the Royal Canadian Mounted Police and CSEC (Communications Security Establishment Canada).

The Harmonized TRA Methodology is designed to address all employees, assets and services at risk. The assessment may be performed at any level of granularity, from broadly based departmental risk profiles to more tightly focused examinations of specific issues.

Departments may want to use the Harmonized TRA (Threat and Risk Assessment) analysis as inputs into the assurance level assessment (Step 1), or they may want to tailor the methodology to develop a targeted and comprehensive TRA (Threat and Risk Assessment) that is used in conjunction with the assurance level assessment. This latter approach may be useful in addressing the highly specialized threat agents associated with the rapidly evolving online environment and the potential vulnerabilities introduced by newer technologies (e.g., tablets, mobile phones).

4.4 IT Security Guidelines

For guidance on authentication related to IT (Information Technology) systems and electronic service delivery, departments should consult the guidelines published by CSEC (Communications Security Establishment Canada): ITSG (Information Technology Security Guideline - User Authentication Guidance for IT Systems)-31 and ITSG-33 (IT Security Risk Management: A Lifecycle Approach).

Following is an overview of these two guidance documents and a suggested application in conjunction with this guideline.

ITSG (Information Technology Security Guideline - User Authentication Guidance for IT Systems)-31 User Authentication Guidance for IT (Information Technology) Systems

This guideline provides guidance on the design and selection of user authentication solutions.

The selection of an authentication solution is based on satisfying the requirements from the following authentication design requirement categories:

- **Authentication factors:** Defines how many authentication factors are required during the authentication process.
- **Authentication tokens:** Defines which tokens are to be used to perform the authentication process.
- **Cryptographic module validation:** Defines the level of validation required for a cryptographic module-based token.
- **Threat mitigation:** Defines the threats which the authentication process should be capable of protecting against.
- **Event logging:** Defines the properties of event logging required during the authentication process in order to maintain the chain of evidence.

Departments should ensure that the design and selection of an authentication solution corresponds to the assurance level requirements specified by this guidance.

ITSG-33 (IT Security Risk Management: A Lifecycle Approach)IT (Information Technology) Security Risk Management: A Lifecycle Approach

ITSG-33 (IT Security Risk Management: A Lifecycle Approach) provides the framework for the IT (Information Technology) security risk management activities that should be undertaken at both the departmental level and the information system level within departments. This document and its appendices provide guidance on the following areas:

- Departmental IT (Information Technology) security risk management activities;
- Information system security risk management activities;
- Security control catalogue; and
- Security control profiles.

Departments should ensure that the design and selection of an authentication solution is consistent with the overall security assessment and security controls specified by this guidance. Departments may also want to use this guidance to help determine the appropriate compensating factors or other safeguards that may be employed to mitigate risks resulting from the selected authentication options.

4.5 Standards-Based and Federation Protocols

Cyber-Authentication Technology Solutions Interface Architecture and Specification Version 2.0 (CATS2 IA&S)

CATS2 IA&S describes and defines the deployment profile for participation in the Government of Canada cyber-authentication environment. It describes the deployment profile and messaging interface required for credential authentication services. The deployment profile is based on the eGov Profile published by the Kantara Initiative and describes additional requirements and constraints specific to the Government of Canada.

Departments should ensure that they are familiar with CATS2 IA&S because it specifies requirements that have been approved for deployment in the Government of Canada context.

Protocol for Federating Identity

The Treasury Board of Canada Secretariat is currently developing the Protocol for Federating Identity. This document will support the Standard on Identity and Credential Assurance and provide the detailed criteria for formally participating in the Government of Canada federation.

5.0. Additional Information

5.1 Next Review Date

This document will be reviewed and updated as required.

5.2 Enquiries and Comments

For enquiries regarding this policy instrument, please contact the Security and Identity Management Division.

6.0. References

Government of Canada References

- Canada Evidence Act
- Common Services Policy
- Directive on Electronic Authentication and Authorization of Financial Transactions
- Directive on Identity Management
- Directive on Privacy Impact Assessment
- Federating Identity Management in the Government of Canada: A Backgrounder
- Framework for the Management of Risk
- Harmonized Threat and Risk Assessment (TRA) Methodology
- Information Technology Security Guideline (ITSG (Information Technology Security Guideline - User Authentication Guidance for IT Systems)-31) - User Authentication Guidance for IT (Information Technology) Systems
- ITSG-33 (IT Security Risk Management: A Lifecycle Approach) - IT (Information Technology) Security Risk Management: A Lifecycle Approach
- Personal Information Protection and Electronic Documents Act
- Policy on Government Security
- Policy on Internal Control
- Secure Electronic Signature Regulations

Public Sector, Industry and International References

- Institute for Citizen-Centred Service, Pan-Canadian Assurance Model, March 3, 2010
- National Institute of Standards and Technology, SP (Special Publication) 800-63-1, Electronic Authentication Guideline, December 2011
- Office of Management and Budget, M-04-04. E-Authentication Guidance for Federal Agencies. December 16, 2003
- Organisation for Economic Co-operation and Development, OECD Recommendation on Electronic Authentication and OECD Guidance for Electronic Authentication, June 2007

Appendix A: Assurance Level Requirement Worksheet

Assurance Level Requirement: The minimum level of assurance required to achieve a program objective, deliver a service or execute a transaction.

Program Activity, Service or Transaction:

Assessor:

Date approved:

To determine the level of assurance required, complete the following sentence using the statements in the cells below and check the appropriate boxes: "If the program, activity, service or transaction above is compromised, it could result in..."

Category of Harm	Level 1 Assessment	Level 2 Assessment	Level 3 Assessment	Level 4 Assessment
1. Inconvenience, distress, loss of standing or reputation	An inconvenience, distress or damage to the standing or reputation of any party	A **serious short-term or a limited long-term** inconvenience, distress or damage to the standing or reputation of any party	A **serious long-term** inconvenience, distress or damage to the standing or reputation of any party	A **severe and permanent** inconvenience, distress or damageto the standing or reputation of any party
2. Financial loss	A financial loss	A **minor** financial loss to any party (**Note:** The severity of the loss depends on the impact of the loss on the affected party)	A **major** financial loss to any party (**Note:** The severity of the loss depends on the impact of the loss on the affected party)	An **extreme** financial loss to any party (**Note:** The severity of the loss depends on the impact of the loss on the affected party)
3. Harm to program or to public interest	An adverse effect on any government organization, program, asset or the public interest	A **limited adverse effect** on a government organization (i.e., it can perform its primary function but with reduced effectiveness), program, organizational asset or the public interest	A **serious adverse effect** on a government organization (i.e., it can perform its primary function with significantly reduced effectiveness), program, organizational asset or the public interest	A **catastrophic effect** on a government organization (i.e., it is unable to perform its primary function), program, organizational asset or the public interest

Category of Harm	Level 1 Assessment	Level 2 Assessment	Level 3 Assessment	Level 4 Assessment
4. Unauthorized release of sensitive personal or commercial information	A loss of personal privacy or breach of personal or commercial information	A **limited adverse effect** on an individual or institution due to the loss of confidentiality or breach of privacy resulting from unauthorized release or improper disclosure of sensitive personal or commercial information	A **serious adverse effect** on an individual or institution due to the loss of confidentiality or breach of privacy resulting from unauthorized release or improper disclosure of sensitive personal or commercial information	A **catastrophic effect** on an individual or institution due to the loss of confidentiality or breach of privacy resulting from unauthorized release or improper disclosure of sensitive personal or commercial information
5. Unauthorized release of sensitive government information (non-personal information)	A loss of confidentiality	A **limited adverse effect** on organizational operations and assets due to a loss of confidentiality resulting from the release of sensitive government information to unauthorized parties	A **serious adverse effect** on organizational operations and assets due to a loss of confidentiality resulting from the release of sensitive government information to unauthorized parties	A **catastrophic effect** on organizational operations and assets due to a loss of confidentiality resulting from the release of sensitive government information to unauthorized parties
6. Civil or criminal violations	(Any compromise involving a legal violation is assessed at a minimum of Level 2)	A **violation** that may have **minor consequences**	A **violation** that may have **serious consequences**	A **violation** that may have **exceptionally grave consequences**
7. Personal health and safety	(Any compromise health and safety is assessed at minimum of Level 2)	A **minor** personal injury **not requiring medical attention**	A personal injury **requiring medical attention**	A **serious** personal injury or **death**

Category of Harm	Level 1 Assessment	Level 2 Assessment	Level 3 Assessment	Level 4 Assessment
8. National interest	(Any compromise involving the national interest is assessed at a minimum of Level 2)	A **disadvantage** to the national interest	An **injury** to the national interest	A **serious or exceptionally grave injury** to the national interest
Assurance Level Requirement	**Minimum Level 1** Required if **any** of the above is checked	**Minimum Level 2** Required if **any** of the above is checked	**Minimum Level 3** Required if **any** of the above is checked	**Minimum Level 4** Required if **any** of the above is checked

Appendix B: Examples of Harm

The following table provides examples for each category of harm and assurance level. These examples may be used as part of the assessment process and in addition to the assessment criteria specified in the table on the preceding page

Category of Harm	Level 1	Level 2	Level 3	Level 4
1. Inconvenience, distress, loss of standing or reputation	• Alternatives are available with little or no delay and no additional costs or degradation of service quality • Minor embarrassment	• Alternatives are readily available • Loss of reputation or standing between the principals • Loss of trust or confidence between principals	• Alternatives are not readily available • Loss of reputation or standing beyond the principals (including third parties) • Loss of trust or confidence beyond the principals (including third parties)	• Alternatives are not available • Wide-scale permanent loss of reputation or standing • Wide-scale permanent loss of trust or confidence

Category of Harm	Level 1	Level 2	Level 3	Level 4
2. Financial loss	No financial loss	• Financial loss that has no impact or only an insignificant material impact on the financial standing of an individual or organization • A budgetary impact that may require reallocation of funds but no additional financing	• Loss of a financial amount that has a significant material impact on the financial standing of an individual or organization • A budgetary impact that may require re-allocation of funds and additional financing	• Loss of a financial amount that severely jeopardizes the financial standing of an individual or organization • Financial restructuring may be required
3. Harm to program or to public interest	• No noticeable reduction in effectiveness of a primary function of an organization • No compromise to a critical asset • No loss of public confidence	• Noticeably reduced effectiveness of a primary function of an organization • No compromise to a critical asset • Temporary loss of public confidence	• Significantly reduced effectiveness of a primary function of an organization • Compromise to a critical asset • Long-term loss of public confidence	• Unable to perform primary function of an organization • Major damage to or potential loss of a critical asset • Permanent loss of public confidence

Category of Harm	Level 1	Level 2	Level 3	Level 4
4. Unauthorized release of sensitive personal or commercial information	• No loss of privacy • No increase in public scrutiny or media attention	• Loss of privacy, unwanted surveillance, tracking, monitoring, data profiling or data matching • Loss of confidence in the organization compromised business relationships or decreased competitive standing • Loss of competitive advantage	• Potential inability to fulfill legal or contractual obligations • Damage to business relationships requiring legal remedies	• Disruption of social order or civil unrest • Loss of business continuity • Cessation of business relationships • Market volatility • Loss of authority (e.g., due to intervention external party)
5. Unauthorized release of sensitive government information (non-personal information)	No increase in public scrutiny or media attention	• Loss of public confidence • Increase of public scrutiny or media attention • Diminished program integrity	• Increased oversight (e.g., increased audits, more stringent approval processes) • Temporary revocation of departmental authorities • Compromise to critical asset	• Loss of continuity of critical government services • Erosion or loss of departmental authorities • Major damage to or potential loss of a critical asset • Irreversible damage to public trust

Category of Harm	Level 1	Level 2	Level 3	Level 4
6. Civil or criminal violations	(Any compromise involving a legal violation is assessed at a minimum of Level 2)	• False claims or wrongful actions having minor financial or legal implications and which pertain to the individual only • The violation does not ordinarily require disciplinary, investigative or enforcement action • The violation may result in a summary offence	• False claims or wrongful actions significant financial or legal implications and which may also pertain to third parties (e.g., trustees acting on behalf of the individual) • Violation could require disciplinary, investigative or enforcement action • The violation may result in an indictable offence (e.g., criminal offence)	• False claims or inaccurate representations in relation to services or transactions where the safety and well-being of the individual or other affected parties may be jeopardized • The violation requires disciplinary, investigative or enforcement action • The violation may result in an indictable offence of a serious nature (e.g., terrorism)
7. Personal health and safety	(Any compromise health and safety is assessed at minimum of Level 2)	No physical injury or psychological distress that requires treatment by first-aid personnel or health care professional	A physical injury or psychological distress that requires treatment by first-aid personnel or health care professional	A physical injury or psychological distress that requires an emergency response
8. National interest	(Any compromise involving the national interest is assessed at a minimum of Level 2)	Any issue that may result in a disadvantage to the national interest	Any issue that is reasonably expected to cause injury to the national interest	Any issue that is reasonably expected to cause serious or exceptionally grave injury to the national interest

Footnotes

* "Individual" is an additional term used in this guideline and not defined in the Standard. It is used to mean "a single human being, as distinct from a family or group." [5]

1 In the rest of this guideline, "departments" refers to departments and agencies.

2 The term "harm" is generic and may also be used to refer to terms used in other assessment frameworks, such as "injuries," "impacts," and "consequences."

3 For the purposes of the Standard and this guideline, the following expressions are considered synonymous: "assurance level," "degree of confidence," "confidence level" and "trust level."

4 Pan-Canadian Assurance Model

5 Canadian Oxford Dictionary, 2nd edition, 2004.

6 These indirect impact considerations are usually taken into account as part of a more global risk assessment, such as a corporate risk profile or a comprehensive harmonized threat risk assessment.

7 Depending on the type of provider, a credential assurance level, an identity assurance level, or both, may be provided.

8 "Compensating factors" may be referred to as "compensating controls" in related guidance documents.

ISBN: 978-0-660-09534-9

Date modified: 2012-11-30