Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada

Information Technology Security Guidance

IT Security Risk Management: A Lifecycle Approach

Glossary

ITSG-33 – Annex 5

November 2012

(editorial changes as of 1 April 2013)

Canada

Foreword

Annex 5 (*Glossary*) to *IT Security Risk Management: A Lifecycle Approach* (ITSG-33) is an unclassified publication issued under the authority of the Chief, Communications Security Establishment Canada (CSEC).

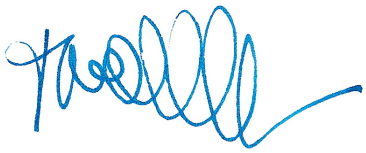
Suggestions for amendments should be forwarded through departmental communications security channels to your Information technology (IT) Security Client Services Representative at CSEC.

Requests for additional copies or changes in distribution should be directed to your IT Security Client Services Representative at CSEC.

For further information, please contact CSEC's IT Security Client Services area by e-mail at itsclientservices@cse-cst.gc.ca, or call (613) 991-7654.

Effective Date

This publication takes effect on 1 November 2012.



Toni Moffa

Deputy Chief, IT Security

Revision History

Document No.	Title	Release Date
ITSG-33 Annex 5	Glossary	1 November 2012
ITSG-33 Annex 5	Grammatical corrections done in some definitions	1 April 2013

Table of Contents

List of Abbreviations and Acronyms

BTEP	Business Transformation Enablement Program
CC	Common Criteria
CSEC	Communications Security Establishment Canada
DDSM	Directive on Departmental Security Management
DSO	Departmental Security Officer
GC	Government of Canada
HTRA	Harmonized Threat and Risk Assessment
ISSIP	Information Security Implementation Process
IT	Information Technology
ITSG	Information Technology Security Guidance
MITS	Management of Information Technology Security
NIST	National Institute of Standards and Technology
PGS	Policy on Government Security
SDLC	System Development Lifecycle
TBS	Treasury Board of Canada Secretariat

1 Introduction

1.1 Purpose

This Annex is part of a suite of guidance documents on information technology (IT) security risk management that the Communications Security Establishment Canada (CSEC) has issued to help Government of Canada (GC) departments and agencies implement, operate, and maintain dependable information systems. This Annex contains the glossary of terms for this suite of guidance documents.

1.2 Publication Taxonomy

This Annex is part of a suite of documents on IT security risk management in the GC. The other documents in the series are as follows:

- ITSG-33, Overview – *IT Security Risk Management: A Lifecycle Approach*
- ITSG-33, Annex 1 – *Departmental IT Security Risk Management Activities*
- ITSG-33, Annex 2 – *Information System Security Risk Management Activities*
- ITSG-33, Annex 3 – *Security Control Catalogue*
- ITSG-33, Annex 4 – *Security Control Profiles*

2 Glossary

a

accidental threat
[menace accidentelle]
An unplanned *threat* caused by a human being. [HTRA, Reference 1]

authorization
[autorisation]
The ongoing process of obtaining and maintaining official management decision by a senior organizational official to authorize operation of an *information system* and to explicitly accept the *risk* of relying on the *information system* to support a set of *business activities* based on the implementation of an agreed-upon set of *security controls*, and the results of continuous *security assessment*. [NIST SP800-39, Reference 7, adapted]

availability
[disponibilité]
The state of being accessible and usable in a timely and reliable manner. [PGS, Reference 2, adapted]

Note:

a) *Availability* is generally applied to information assets, application software, and hardware (infrastructure and its components). *Availability* can also be applied to *business processes*, and personnel.

b) It is implicit in the definition that the *integrity* of objects being accessed has not been *compromised* (e.g., corrupted *data* or *business process* is not considered available, because it is not usable).

availability security objective
[objectif de sécurité lié à la disponibilité]
To ensure the *availability* of a *business activity* or *IT asset* against a specified set of threats in order to prevent *injury* to *national interests* or *non-national interests*.

b

baseline security controls
[contrôles de sécurité de base]
Mandatory *security controls* of Treasury Board of Canada Secretariat (TBS) policy instruments for implementation by *departments* in *departmental IT security functions* and *information systems*. [MITS, Reference 3]

business activity *[activité opérationnelle]*	Any activity performed by a *department* in the course of its operations to deliver or support the delivery of its programs or services. A *business activity* is composed of one or several *business processes* and related *information assets*. Note: A *business activity* can be a GC program (e.g., Employment Insurance), a specific *business process* and related *information assets* (e.g., accounting), or a set of *business processes* and related *information assets* with common organizational objectives (e.g., human resources management). *Business activities* can also include broader concerns such as mission, image, and reputation.
business context *[contexte opérationnel]*	A component of a *departmental* or *domain security control profile*. A *business context* defines the *business activities* that are within the scope of a profile in terms of their *business processes*, related *information assets*, *business needs for security*, and their *security categories*.
business domain *[domaine opérationnel]*	An operational environment where a *department* performs *business activities* supporting common organizational objectives.
business domain security control profile (domain security control profile) *[profil de contrôle de sécurité de domaine opérationnel]*	A *departmental security control profile* for a specific *business domain* as opposed to a *department* as a whole.
business need for security *[besoin opérationnel en matière de sécurité]*	Any protection or compliance requirement associated with a *business activity* that can be satisfied by *security controls*. *Business needs for security* are derived from laws (e.g., Employment Insurance Act, Financial Administration Act), policies (e.g., Policy on Financial Management, Information and Reporting), and any other regulatory instruments such as directives and standards governing GC *business activities*. *Business needs for security* can also be derived from departmental missions, objectives, priorities, the need to preserve the organization's image and reputation, and various obligations that may have been contracted.
business process *[processus opérationnel]*	A *business process* refers to the work required to transform inputs into outputs. [BTEP, Reference 4, adapted from *service process*]

c

classified IT asset *[bien de TI classifié]*	An *IT asset* that contains, stores, processes, or transmits *data* representing information that may qualify for an exemption or exclusion under the *Access to Information Act* or the *Privacy Act*, because its disclosure would reasonably be expected to cause *injury* to *national interests*.

compromise
[compromission]

noun. The unauthorized access to, disclosure, destruction, removal, modification, use, or interruption of *IT assets,* causing a loss of *confidentiality*, *integrity* and/or *availability.* [PGS, Reference 2, adapted]

verb. The act of causing a *compromise* by exploiting *vulnerabilities*.

Note: This loss may lead to the failure of a *business activity* and its related requirements. This failure may lead to *injuries* to *national interests* or *non-national interests*.

confidentiality
[confidentialité]

The state of being disclosed only to authorized *principals*. [PGS, Reference 2, adapted]

Note: *Confidentiality* is typically applied to *information assets*. *Confidentiality* can also be applied, usually at a classified level, to some *business activities*, such as military missions and intelligence collection activities, where the fact the mission or activity exists is classified, and the particulars of its execution is also classified. Operations Security (OPSEC), typically supported by *IT security*, is one technique used to protect the *confidentiality* of *business activities*. In addition, *confidentiality* can also be applied to other types of *IT assets* such as Type-1 COMSEC and SIGINT equipment or weapons systems. *Confidentiality* in these cases means that the equipment must be provided to, handled by, and disposed of by cleared and authorized personnel. An adversary getting hold of classified equipment may be able to reverse engineering it to deduce classified information about the design, configuration, and weaknesses.

confidentiality security objective
[objectif de sécurité lié à la confidentialité]

To ensure the *confidentiality* of *business activities* and *IT assets* against a specified set of *threats* in order to prevent *injury* to *national interests* or *non-national interests*.

confirm
[confirmer]

Declare that something has been reviewed in detail with an independent *determination* of sufficiency. [CC, Reference 5]

critical IT asset
[bien de TI essentiel]

An *IT asset* that supports a *business activity* having some degree of *criticality*.

criticality
[criticité]

The relative importance of a *business activity* in promoting or maintaining the health, safety, security, or economic well-being of Canadians, or to the effective functioning of the GC. [PGS, Reference 2, adapted from critical service]

d

data
[données]

Electronic representation of *information*. The quantities, characters, or symbols on which operations are performed by a computer, being stored and transmitted in the form of electrical signals and recorded on magnetic, optical, or mechanical recording media. [Oxford, Reference 9, adapted]

deliberate threat *[menace délibérée]*	A planned or premeditated *threat* caused by a human being. [HTRA, Reference 1]
demonstrate *[démontrer]*	Provide a conclusion gained by an analysis that is more rigorous than a *trace* but less rigorous than a proof. To *demonstrate* a mapping, a rigorous analysis and an informal proof of the more detailed correspondence between elements of successive specifications is required. [CC, Reference 5]
departmental security control profile *[profil de contrôle de sécurité ministériel]*	A set of *security controls* that a *department* establishes as the minimum mandatory requirements for their *departmental IT security function* and their *information systems*. A profile must satisfy TBS *baseline security controls* and departmental *business needs for security* with due consideration for the departmental *threat context* and *technical context*.
departmental security program *[programme de sécurité ministérielle]*	The group of security-related resource inputs and activities that departmental security officers (DSOs) manage to address the security needs of their *department* while achieving the results set forth in security-related TBS policy instruments. [DDSM, Reference 6] adapted from *security program*]
departmental security requirement *[exigence de sécurité ministérielle]*	Any *security requirement* prescribed by senior officials of a *department* that applies generally to *information systems* of that *department*. *Departmental security requirements* may relate to *business processes*, *information assets*, IT-related *threats*, *robustness levels*, *security control profiles*, *security assurance* requirements, *business needs for security*, *security architecture*, security design, common *security controls*, and specific *security solutions*.
departments (GC departments) *[ministères]*	GC *departments*, agencies, and other organizations subject to the *Policy on Government Security*.
describe *[décrire]*	Provide specific details. [CC, Reference 5]
determine *[déterminer]*	Affirm a particular conclusion based on independent analysis with the objective of reaching a particular conclusion. [CC, Reference 5]
development environment *[environnement de développement]*	Environment in which the *information system* is developed. [CC, Reference 5, adapted]

e

enterprise architecture
[architecture d'entreprise]

A description of the structure of an enterprise, which comprises enterprise components (business entities), the externally visible properties of those components, and the relationships (e.g. the behaviour) between them. *Enterprise architecture describes* the terminology, the composition of enterprise components, and their relationships with the external environment, and the guiding principles for the requirement, design, and evolution of an enterprise. This description is comprehensive, including enterprise goals, *business processes*, roles, organizational structures, organizational behaviours, business *information*, software applications, and *information systems*. [Wikipedia, March 2011, adapted]

enterprise architecture program
[programme d'architecture d'entreprise]

The set of resources, plans, policies, processes, procedures, and tools that a *department* allocates and implements to coordinate and manage the development and maintenance of an *enterprise architecture*.

i

implementation (implement, implementing)
[mise en œuvre (mettre en œuvre)]

A term used to designate the phases of the *system lifecycle* that are responsible for the delivery of an *information system*. It includes the initiation, development/acquisition, and integration and installation phases of the *system lifecycle*, but excludes the operations and maintenance phase and the disposal phase.

implementation representation
[représentation de la mise en œuvre]

The least abstract representation of an *information system*. It consists of source code, hardware and software products, physical network diagrams, configuration documentation such as build books, and so on. Collectively, these elements allow for the construction of the *information system* without having to make any further design or *implementation* decisions.

information (information asset)
[information (biens d'information)]

Any pattern of symbols or sounds to which meaning may be assigned. [HTRA, Reference 1]

information system
[système d'information]

An *information system* is generally composed of *data*, computing platforms, communications networks, business applications, people, and processes, organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of *information*. [NIST SP800-39, Reference 7, adapted]

information system security implementation process (ISSIP) *[processus d'application de la sécurité dans les systèmes d'information (PASSI)]*	The process of identifying security needs and then building *information systems* capable of satisfying these needs in a real-world operational environment. *ISSIP* incorporates process areas of *information system* security engineering, *security assessment*, and *authorization* to form a comprehensive process for the *implementation* of dependable *information systems*.
injury *[préjudice]*	The damage to the *national interests* and *non-national interests* that *business activities* serve resulting from the *compromise* of *IT assets*. [HTRA, Reference 1, adapted]
injury level *[niveau de préjudice]*	The severity of an *injury*. Five levels are defined: very low, low, medium, high, very high.
integrity *[intégrité]*	The state of being accurate, complete, authentic, and intact. [DDSM, Reference 6] Note: Integrity is generally applied to *information assets*. Integrity can also be applied to *business processes*, software application logic, hardware and personnel.
integrity security objective *[objectif de sécurité lié à l'intégrité]*	To ensure the *integrity* of a *business activity* or *IT asset* against a specified set of *threats* in order to prevent *injury* to *national interests* or *non-national interests*.
IT asset *[bien TI]*	A generic term used to represent business applications, electronic representations of *information* (*data*), and the hardware, software, and system *data* that *information systems* are composed of.
IT security *[sécurité des TI]*	The discipline of applying *security controls*, *security solutions*, tools, and techniques to protect *IT assets* against *threats* from *compromises* throughout their *lifecycle*, based on the *security category* of supported *business activities*, and in accordance with *departmental* and GC policies, directives, standards, and guidelines. Note: Protecting *IT assets* helps protect departmental *business activities* and therefore departmental mission and objectives.
IT security function *[fonction de sécurité des TI]*	The elements of a *departmental security program* that are dedicated to the protection of departmental *IT assets*.
IT security incident *[incident lié à la sécurité des TI]*	Any unexpected or unwanted event that might cause a *compromise* of *IT assets*. [MITS, Reference 3, adapted]
IT security risk *[risque lié à la sécurité des TI]*	The potential that a given *threat* will *compromise IT assets* and cause *injury*. [HTRA, Reference 1, adapted]

IT security risk management *[gestion des risques liés à la sécurité des TI]*	The process by which organizations manage *IT security risks*. *IT security risk management* is achieved through *IT security* and other risk management processes.
IT threat *[menace liée à la sécurité des TI]*	Any potential event or act, *deliberate*, *accidental* or *natural hazard,* that could *compromise IT assets*. [HTRA, Reference 1, adapted]

j

justify (justification) *[justifier (justification)]*	Provide a conclusion gained by an analysis that is more rigorous than a demonstration but less rigorous than a proof. It requires significant rigour in terms of very carefully and thoroughly explaining every step of a logical argument. [CC, Reference 5, adapted from justification]

m

management security control *[contrôle de sécurité de gestion]*	A *security control* that focuses on the management of *IT security* and *IT security risks*. [NIST FIPS 200, Reference 11, adapted]
monitor (monitoring) *[surveiller (surveillance)]*	The continuous process of observing the operations of *information systems* with the objective of detecting deviations from planned or expected behaviour.
must *[doit]*	This word means that the statement is a mandatory requirement. [RFC 2119, Reference 8, adapted]

n

natural hazard *[risque naturel]*	A *threat* attributable to forces of nature. [HTRA, Reference 1]
national interests *[intérêts nationaux]*	The security and the social, political, and economic stability of Canada. [PGS, Reference 2]
non-national interests *[intérêts non nationaux]*	The safety, health, and well being of individuals, and the financial position and reputation of individuals and Canadian companies. [PGS, Reference 2, SOAS, Reference 10, adapted]

o

operational security control
[contrôle de sécurité opérationnel]
A *security control* that is primarily implemented and executed by people and is typically supported by the use of technology, such as supporting software. [NIST FIPS 200, Reference 11, adapted]

p

principal
[mandant]
Participating entity in an *information system* (physical person, legal person, role, equipment, channel, automated process).

protected IT asset
[bien de TI protégé]
An *IT asset* that contains, stores, processes, or transmits *data* representing *information* that may qualify for an exemption or exclusion under the *Access to Information Act* or the *Privacy Act* because its disclosure would reasonably be expected to cause *injury* to *non-national interests*. [DDSM, Reference 6, adapted]

r

recommended
[recommandé(e)]
Refer to the definition of *should*.

residual risk (IT security residual risk)
[risque résiduel (risque résiduel lié à la sécurité des TI)]
A *risk* that remains after *security controls* have been selected, approved and implemented. [HTRA, Reference 1, adapted]

Note: Business owners should generally require the support of an *information system* with a *security posture* that aligns with their tolerance to *risk*. For example, they should require the support of an *information system* with a *strong security posture* where their tolerance to *risk* is low. However, this may not always be the case. For example, it may be acceptable for troops to deploy in theatre to save lives with the support of *IT assets* having a weaker *security posture* than would normally be required if the consequences of not performing the mission (i.e., loss of many civilian lives) are worse (relatively) than the consequences of relying on these IT assets of weaker security posture to perform the mission (i.e., loss of some military assets).

residual risk level (IT security residual risk level)
[niveau de risque résiduel (niveau de risque résiduel lié à la sécurité des TI)]
The degree of *residual risk*.

residual risk assessment *[évaluation du risque résiduel]*	The assessment performed at the conclusion of the *system development lifecycle* to adjust the conclusions of the detailed *threat and risk assessment* to account for unresolved security deficiencies identified during the design, development, testing, and installation phases.
risk *[risque]*	Refer to the definition of *IT security risk*.
risk level *[niveau de risque]*	The degree of *risk*. Note: The degrees are usually labeled: very low, low, medium, high, very high. The definition of those labels depends on the risk assessment methodology.
robustness *[robustesse]*	A characterization of the *security strength* and *security assurance* of an implemented *security control*.
robustness level *[niveau de robustesse]*	A robustness level is composed of a *security strength* component and a *security assurance* component. Together, these two components define the requirements that must be met in the implementation and operation of a *security control* to satisfy defined *security control objectives*. Note: A *security control* of a higher robustness level aims to counter *threat agents* with more sophisticated capabilities, or *accidental threats* and *natural hazards* of higher magnitude.

S

security architecture *[architecture de sécurité]*	The elements of *enterprise architecture* that relate to *IT security*.
security assessment *[évaluation de sécurité]*	The ongoing process of evaluating the performance of *IT security controls* throughout the *lifecycle* of *information systems* to establish the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the departmental *business needs for security*. *Security assessment* supports *authorization* by providing the grounds for confidence in *information system* security. [NIST SP800-39, Reference 7, adapted from *security control assessment*]
security assurance *[assurance de la sécurité]*	Confidence-building tasks that aim to ensure that a *security control* is designed and implemented correctly, and is operating as intended. In addition, *security assurance* includes tasks that aim to ensure the ability of all *security controls* in an *information system*'s security design, implementation and operations to satisfy the *security requirements*.
security assurance level *[niveau d'assurance de la sécurité]*	The level of assurance achieved by completing a predefined set of *security assurance tasks*.

security assurance task *[tâche liée à l'assurance de la sécurité]*	An action performed by a security practitioner or an assessor to establish assurance (confidence) in a specific security aspect of an *information system*. There are two types of *security assurance tasks*: engineering task and assessment task. Engineering tasks include the production of documentation and may need to satisfy documentation content requirements.
security categorization *[catégorisation de la sécurité]*	The process of determining the *security category* of *business activities*, *information systems*, and *IT assets*. Notes: a) *Security categorization* is established by assessing *injury* to *national* and *non-national interests* as a result of failures of *business activities* to meet their *security objectives of confidentiality, integrity, and availability*. *Information systems* and *IT assets* generally inherit the *security category* of the *business activities* that relate to them. b) At the departmental level, *security categorization* is a continuous activity for categorizing the security of *business activities* to support the development of *security control profiles*. At the *information system* level, *security categorization* is an activity of the ISSIP for categorizing the security of the *information system* and its *IT assets*. For the *information system*, it is done early in the *system development lifecycle*. For *IT assets*, it is done later during the design phases when *IT assets* have been defined.
security category *[catégorie de sécurité]*	A *security category* characterizes a *business activity* by the severity of expected *injuries* (*injury level*) from *compromise* with respect to the *security objectives* of *confidentiality*, *integrity*, and *availability*.
security control (IT security control) *[contrôle de sécurité (contrôle de sécurité des TI)]*	A management, operational, or technical high-level security requirement prescribed for an *information system* to protect the *confidentiality*, *integrity*, and *availability* of its *IT assets*. *Security controls* are implemented using various types of security solutions that include security products, security policies, security practices, and security procedures. [NIST SP800-39, Reference 7, adapted]
security control enhancement *[amélioration des contrôles de sécurité]*	A statement of security capability to: (i) build in additional, but related, functionality to a basic control; and/or (ii) increase the *security strength* of a basic *security control*. [NIST SP800-39, Reference 7]

security control objective
[objectif en matière de contrôles de sécurité]

A statement, stated in a standardize language, that formalizes what is to be achieved by a *security control* to satisfy *business needs for security*.

Note: A *security control objective* should be written in a way that is specific, measurable, attainable, results-oriented, and time-based. A *security control objective* must be measurable using performance metrics, continuous *monitoring*, and *security assessment*.

The implementation of security controls aims to fulfill the *security control objectives*, in order to satisfy the *business needs for security*. For example, the issuance of an accurate benefits amount to an authorized recipient (citizen) is a *business need for security*. The *security control objectives* for this *business need for security* may be defined as a function of the positive authentication of the recipient with a defined error rate; the positive authorization of the recipient in receiving the benefits payment with a defined error rate; and the preservation of the *integrity* of the payment transaction event (log of the *business process* events) and payment record (log of the approved payment and all related *information*) with high confidence.

The exact metrics (e.g., error rate and confidence) associated with the *security control objectives* need to be defined based on the *injuries* that could be incurred by the recipient where the *business need for security* is not satisfied.

The metrics may be loose when the *injuries* are minor (an inaccurate payment amount leads to some inconvenience), or strict when the *injuries* are serious (an inaccurate amount leads to serious stress and financial loss).

security measure
[mesure de sécurité]

Refer to the definition of *security solution*.

security mechanism
[mécanisme de sécurité]

A class of *security solutions* rated in terms of *security strength* of protection and *security assurance* of implementation to address specific *threats*.

Note: examples of classes of *security solutions* are: biometrics, digital signature, hot standby, anti-tampering, discretionary access control, packet filtering. Each of these classes can be implemented by various *security solutions* (e.g., products). For example, biometrics can be implemented using fingerprint, iris or retina scanners.

security objective
[objectif de sécurité]

Refer to the definitions of *confidentiality security objective*, *integrity security objective,* and *availability security objective*.

security posture [posture de sécurité]

A characteristic of an *information system* that represents its resilience to a specific set of deliberate attacks and accidental and natural hazards (i.e., *selected threats*)

Note: Resilience relates not only to the capability of the *information system* to prevent *threats* but also to detect, respond, and recover from their *compromises*. A security posture is assessed without regard for *unselected threats*.

security posture (very weak) *[posture de sécurité (très faible)]*

This rating means that the potential for *selected threats compromising* an *information system*'s *IT assets* is assessed as **severe**. This rating indicates that the *information system* has not been adequately built to prevent, detect, respond, or recover from *compromises*. The *department* does not have in place the mechanisms to manage *IT security incidents* and *compromises*, or to implement required improvements.

security posture (weak) *[posture de sécurité (faible)]*

This rating means that the potential for *selected threats* compromising an *information system*'s *IT assets* is assessed as **considerable**. Issues characterizing an *information system* having a *weak security posture* typically include many of the following:

1. The *business needs for security* are not fully understood and are not well documented;
2. The *security controls* and *requirements* are not fully defined and are not well documented;
3. The *threats* are not fully understood and are not well documented;
4. The implemented *security solutions* fulfill only partially the *security controls* and *requirements*, without adequate *assurance*;
5. The *information system* is not operated in a manner to maintain the *security posture*;
6. The *departmental IT security function* does not perform adequate *monitoring* and *security assessment*;
7. The *department* does not have mechanisms in place to learn from the *IT security incidents* and *compromises* and to implement required improvements.

These elements increase the potential of *threats compromising IT assets* due an increase in the number or significance of exploitable *vulnerabilities*. In the event of a *compromise*, the *information system*, IT operations group, and the *departmental IT security function* cannot **effectively** detect, respond to, and recover from the *compromise*.

security posture (average) *[posture de sécurité (moyenne)]*

This rating means that the potential for *selected threats compromising* an *information system*'s *IT assets* is assessed as **significant**. Issues characterizing an *information system* having an *average security posture* may include some of the following:

1. The *business needs for security* are not fully understood or are not well documented;
2. The *security controls* and *requirements* are not fully defined or are not well documented;
3. The *threats* are not fully understood or are not well documented;
4. The implemented *security solutions* fulfill only partially the *security controls* and *requirements*, without adequate *assurance*;
5. The *information systems* is not operated efficiently in a manner to maintain the security posture;
6. The *departmental IT security function* does not perform efficient *monitoring* and *security assessment*;
7. The *department* does not have in place mature mechanisms to learn from *IT security incidents* and *compromises* and to implement required improvements.

These elements increase the potential of *threats compromising IT assets* due an increase in the number or significance of exploitable *vulnerabilities*. In the event of a *compromise*, the *information system*, IT operations group, and the *departmental IT security function* cannot **gracefully** detect, respond to, and recover from the *compromise*.

security posture (strong)
[posture de sécurité (solide)]

This rating means that the potential for *selected threats compromising* an *information system*'s *IT assets* is assessed as **minor**. The key characteristics of an information system having a *strong security posture* include most or all of the following:

1. The *business needs for security* are well understood and documented;
2. The *security controls* and *requirements* are well defined and documented;
3. The *threats* are well understood and documented;
4. The implemented *security solutions* fulfill the *security controls* and *requirements*, with adequate *assurance*;
5. The *information system* is operated in a manner to maintain the *security posture* over time;
6. The *departmental IT security function* performs adequate *monitoring* and *security assessments* of implemented *security controls*;
7. In the event of a *compromise*, the *information system*, IT operations group, and the *departmental IT security function* can detect, respond to, and recover gracefully from the *compromise*, thus minimizing the possibility of incurring *injuries*, or the severity of *injuries*;
8. The *department* learns from *incidents* and implements any required improvements.

This rating indicates that the *information system* has been adequately built to prevent, detect, respond, and recover **gracefully** from *compromise*.

security posture (very strong)
[posture de sécurité (très solide)]

This rating means that the potential for *selected threats compromising* an *information system*'s *IT assets* is assessed as **very small**. The *information system* fully satisfies *business needs for security*, has been adequately built to prevent, detect, respond, and recover **gracefully** from *compromise*, and is fully documented. The *department* has in place mature mechanisms to manage incidents and *compromise*, learns from the experience, and implements required improvements promptly.

security requirement
[exigence de sécurité]

Any need, stated in a standardized language, that an *information system* must satisfy through *IT security* that contributes to achieving a *business need for security*. [CC, Reference 5, adapted]

security safeguard
[mesure de protection de la sécurité]

Refer to the definition of *security solution*.

security solution *[solution de sécurité]*	Any security function, product, practice, or procedure that is implemented in an *information system* to realize a *security control*.
security strength *[force de la sécurité]*	The characterization of an implemented *security control*'s potential to protect *IT assets* against *compromises* from *threats*. Note: As the *security strength* increases, the effort (cost) or magnitude required by the *threat agent* to defeat the implemented *security control* also increases. The protective potential of an implemented *security control* can be fulfilled only when it is implemented with adequate *security assurance*.
security testing *[test de sécurité]*	Testing conducted during the development phase and the integration and testing phase of the *system development lifecycle* (SDLC) and that contributes to the establishment of *security assurance*. Note: During the development phase, *security testing* includes functional testing of custom security solutions (e.g., functional unit testing) and may also include other forms of testing such a negative functional testing of non-security functions (e.g., fuzz testing of URL against a web application) and the testing of operational procedures to *determine* usability and maintainability. During the integration and testing phase, *security testing* includes functional *security testing* and may also include *vulnerability assessments* and penetration testing, depending on the *security assurance* requirements.
selected threat (selected IT threat) *[menace sélectionnée (menace sélectionnée liée à la sécurité des TI)]*	Any IT-related *threat* that has been deemed, through a *threat assessment*, as relevant to a *business activity* or an *information system* and against which a *department* intends to protect its *IT assets*. Note: Factors influencing the selection of *threats* include, for example, the resources and skill set available or not available to the organization to effectively counter a *threat*; the limited budget allocated to *IT security*; the assessment that some *threat compromises* may not lead to *injuries*; etc. Refer to the definition of *threat assessment* for more information.
shall *[doit]*	Refer to the definition of *must*.
should *[recommandé(e)]*	This word indicates a goal or preferred alternative. There may exist valid reasons in particular circumstances to ignore a particular item or statement, but the full implications must be understood and carefully weighed before choosing a different course. [RFC 2119, Reference 8, adapted]
statement of assessment *[énoncé d'évaluation]*	Any recognition or acknowledgement that the assessment process has been completed with acceptable results. It can be as simple as a record of decision appearing in the minutes of an engineering or project meeting or as formal as an assessment certificate signed by a security assessor.

system development lifecycle *[cycle de développement des systèmes]*	The successive stages through which *information systems* are implemented (i.e., brought into service or delivered). Note: The reference SDLC used in ITSG-33 publications consists of the following phases: 1) stakeholder engagement, 2) concept, 3) planning, 4) requirements analysis, 5) high-level design, 6) detailed design, 7) development, 8) integration and testing, and 9) installation.
system lifecycle *[cycle de vie des systèmes]*	The successive stages that *information systems* pass through from their inception to their end of life. Note: The reference SLC used in ITSG-33 publications consists of the following phases: 1) Initiation, 2) development/acquisition, 3) integration and installation, 4) operations and maintenance, and 5) disposal.

t

technical context *[contexte technique]*	A component of a *departmental or domain security control profile*. A *technical context* defines in general terms the technical environment that might influence the selection of the profile's *security controls*.
technical security control *[contrôle de sécurité technique]*	A *security control* implemented and executed by *information systems* primarily through *security mechanisms* contained in hardware, software, and firmware components. [NIST FIPS 200, Reference 11, adapted] Note: A *technical security control* is dependent on the proper functioning of the *information system* for effectiveness. Also, some operational aspects may be included in the *implementation* of the control (e.g., manual assessment of log monitoring results).
threat *[menace]*	Refer to the definition of *IT threat*.
threat agent *[agent de menace]*	An identifiable organization, individual or type of individual posing *deliberate threats*, or a specific kind of *accidental threats* or *natural hazard*. [HTRA, Reference 1]
threat assessment (IT-related threat assessment) *[évaluation des menaces (évaluation des menaces liées à la sécurité des TI)]*	The process of identifying and qualifying *threats* faced by an organization's *business activities* and *information systems* supporting them. Note: A threat assessment will identify all *threats* faced by an organization. The *selected threats* are the ones that the organization chooses to address and are documented explicitly. *Threats* that an organization may face, but that are not addressed for various reasons, such as cost constraints, technical constraints, or operational constraints, are also documented explicitly (i.e., unselected *threats*).

threat and risk assessment (IT-related TRA) *[évaluation des menaces et des risques (EMR liée aux TI)]*	The process of identifying and qualifying *threats* and *risks* to *IT assets* and of implementing or recommending additional *security controls* to mitigate *risks* that are deemed unacceptable.
threat context *[contexte de menace]*	A characteristic of a *departmental or domain security control profile*. A *threat context* defines the *selected threats* of relevance to the domain's *business activities*.
threat event *[incident]*	An actual incident in which a *threat agent* exploits a *vulnerability* with potentially adverse effects on an *IT asset* of value. [HTRA, Reference 1, adapted]
trace (tracing) *[tracer (traçabilité)]*	Perform an informal correspondence analysis between two entities with only a minimal level of rigour. Tracing involves documenting a basic correspondence between the elements of successive specifications.

V

vulnerability *[vulnérabilité]*	An attribute of an *IT asset* or the environment in which it is located (including the *security solutions*) that increases the likelihood of a *threat event*, the probability of *compromise* or the severity of the outcome. *Vulnerabilities* are inversely proportional to *security solutions* effectiveness. [HTRA, Reference 1, adapted]
vulnerability assessment *[évaluation des vulnérabilités]*	A *determination* of the existence of *information system vulnerabilities*. [MITS, Reference 3]

3 References

[Reference 1] Communications Security Establishment Canada and the Royal Canadian Mounted Policy. *Harmonized Threat and Risk Assessment (TRA) Methodology*. 23 October 2007.

[Reference 2] Treasury Board of Canada Secretariat. *Policy on Government Security*. 1 July 2009.

[Reference 3] Treasury Board of Canada Secretariat. *Operational Security Standard: Management of Information Technology Security*. 31 May 2004.

[Reference 4] Treasury Board of Canada Secretariat. Business Transformation Enablement Program (BTEP). Glossary. April 2006.

[Reference 5] *Common Criteria for Information Technology Security Evaluation Part 3: Security Assurance Requirements*. CCMB-2009-07-001, Version 3.1, Revision 3. July 2009.

[Reference 6] Treasury Board of Canada Secretariat. *Directive on Departmental Security Management*. 1 July 2009.

[Reference 7] National Institute of Standards and Technology. Information Security. *Managing Information Security Risk: Organization, Mission, and Information System View*. NIST Special Publication 800-39, March 2011.

[Reference 8] Internet Engineering Task Force. RFC2119 *Key words for use in RFCs to Indicate Requirement Levels*. March 1997.

[Reference 9] Oxford Dictionaries Online (ODO). http://oxforddictionaries.com

[Reference 10] Treasury Board of Canada Secretariat. *Security Organization and Administration Standard*. 1 June 1995.

[Reference 11] National Institute of Standards and Technology. *Minimum Security Requirements for Federal Information and Information Systems* FIPS PUB 200. March 2006.