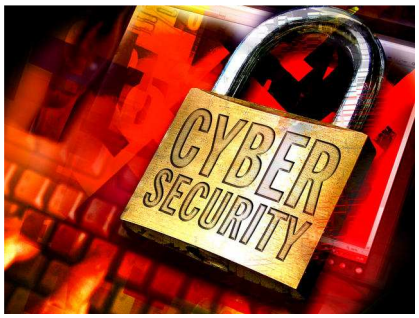
GLOSSARY



Acceptable Level of Risk - A judicious and carefully considered assessment by the appropriate Designated Approving Authority that an information technology (IT) activity or network meets the minimum requirements of applicable security directives. The assessment should take into account the value of IT assets; threats and vulnerabilities; countermeasures and their efficiency in compensating for vulnerabilities; and operational requirements.

Accountability - The property that ensures that the actions of an entity may be traced uniquely to that entity.

Accreditation – A formal declaration by the responsible management authority approving the operation of an automated system in a particular security mode using a particular set of safeguards. Accreditation is the official authorization by management for the operation of the system, and acceptance by that management of the associated residual risks. Accreditation is based on the certification process as well as other management considerations.

Attack - The act of aggressively trying to bypass security controls on an IT system or network. The fact that the attack is made does not mean it will succeed. The success depends on the vulnerability of the system, network or activity and the effectiveness of the safeguards in place.

Availability - The accessibility of systems, programs, services and information to authorized users when needed and without undue delay.

Baseline - An element of a system that cannot be changed without formal approval.

Classification - A determination that information requires a specific degree of protection against unauthorized disclosure together with a designation signifying that such a determination has been made.

Compromise - A violation of the security policy of a system or network such that an unauthorized disclosure, modification, removal, interruption or destruction of sensitive information may have occurred.

Computer Security - The protection resulting from measures designed to prevent deliberate or inadvertent unauthorized disclosure, acquisition, manipulation, destruction, modification, or loss of information contained in a computer system, as well as measures designed to prevent denial of authorized use of the system.

Confidentiality - The property that information is not made available or disclosed to unauthorized individuals, entities, or processes.

Exposure - The degree to which an asset or group of assets may be exposed to loss, disclosure, destruction or modification, or possibly to undesirable consequences, by the occurrence of one or more threat events.

Department (ministère) – any federal institution subject to the Security policy.

Impact - A measure of the degree of damage or other change caused by a threat event.

Information Technology Security (ITS) - The protection resulting from an integrated set of safeguards designed to ensure the confidentiality of information electronically stored, processed or transmitted; the integrity of the information and related processes; the accountability of the information stored, processed or transmitted; and the availability of systems and services.

IT Security Policy - Rules, directives and practices that govern how assets, including sensitive information, are managed, protected and distributed within an organization and its IT systems

Integrity - The accuracy and completeness of information and assets and the authenticity of transactions.

Lead agency (organisme conseil) – an agency with government wide responsibilities related to the Security policy, as defined in the Security policy.

Loss - A quantitative measure of harm or deprivation resulting from a compromise.

Managed Risk - Attained when the extent of security protection is commensurate with the cost of implementing security measures and the risk: the likelihood of a breakdown in security and the impact that it would have on a program.

Monitor or Monitoring - To ensure that information and assets, or the safeguards protecting them, are checked by the personnel in control of the information or assets, by security staff or by electronic means with sufficient regularity to satisfy the threat and risk assessment.

Personal Information - Any form of recorded information about an identifiable individual. Personal information, a subset of other sensitive information, deserves enhanced protection.

Personnel Security - The procedures established to ensure that all personnel who have access to any sensitive information have the required authorities as well as all appropriate clearances.

Physical Security - The application of physical barriers and control procedures to provide protection, detection and response mechanisms used in the physical environment to control access to sensitive information and assets.

Privacy - The right of individuals to control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed. Note: Because this term relates to the right of individuals, it cannot be very precise and its use should be avoided except as a motivation for requiring security.

Risk - Intuitively, the adverse effects that can result if a vulnerability is exploited or if a threat is actualized. In some contexts, a risk is a measure of the likelihood of adverse effects or the product of the likelihood and the quantified consequences. There is no standard definition. (Based on Computer Related Risks)

Risk Assessment - An evaluation of risk based on threat assessment information, the effectiveness of existing and proposed security safeguards, the likelihood of system vulnerabilities being exploited and the consequences of the associated compromise to system assets.

Risk Management - The process by which resources are planned, organized, directed, and controlled to ensure the risk of operating a system remains within acceptable bounds at optimal cost.

Safeguard(s) - The approved minimum security measure(s) and controls which, when correctly employed, will prevent or reduce the risk of exploitation of specific vulnerability(ies) which would compromise an IT system.

Security Audit - An independent review and examination of system records and activities in order to test for adequacy of system controls, to ensure compliance with established security policy and operational procedures, to detect breaches in security, and to recommend any indicated changes in control, security policy and procedures.

Security Requirement(s) - The specification of a security function(s) needed within an IT system, which if satisfied will result in the IT system meeting its Target Residual Risk.

Security standard (normes de sécurité) – level of attainment regarded as a measure of adequacy; security requirements and guidelines approved for government wide use. (Operational standards form part of the Treasury Board Manual; technical standards are produced by the lead security agencies).

System Certification - The comprehensive assessment of the technical and non technical security features of an information system/network and other safeguards, made as part of and in support of the accreditation process, that establishes the extent to which a particular design and implementation meets a specific set of security requirements. Certification evidence provided must satisfy accreditation requirements and all certification activities must be completed before the accreditation can be finalized.

Threat - Any potential event or act that could cause one or more of the following to occur: unauthorized disclosure, destruction, removal, modification or interruption of sensitive or critical information, assets or services. A threat can be natural, deliberate or accidental.

Threat Assessment - An evaluation of threat agent characteristics including resources, motivation, intent, capability, opportunity, likelihood and consequence of acts that could place sensitive information and assets at risk.

Threat and Risk Assessment (TRA) - A process in which the objective is to identify system assets, to identify how these assets can be compromised by threat agents, to assess the level of risk that the threat agents pose to the assets and recommend the necessary safeguards in order to mitigate effects of the threat agents. Also, see Threat Assessment and Risk Assessment.

Vulnerability - A quantifiable, threat-independent characteristic or attribute of any asset within a system boundary or environment in which it operates and which increases the probability of a threat event occurring and causing harm in terms of confidentiality, availability and/or integrity, or increases the severity of the effects of a threat event if it occurs.