Government of Canada

Information Technology Incident Management Plan

Catalogue No.
ISBN

This document is available on the Treasury Board of Canada Secretariat
Web site at www.tbs-sct.gc.ca

This document is available in alternative formats

Document Revision History

Date	Version	Comments addressed (or source)	Author

Preface

The occurrence of information technology (IT) and IT security (ITS) incidents involving Government of Canada (GC) networks and infrastructure can have a significant impact on government operations, services delivered to Canadians, and, consequently, confidence in government. To provide timely and efficient management of incidents, an incident management program must have supporting services, activities, and strategic leadership in place to ensure informed decision making.

The Government of Canada IT Incident Management Plan (GC IT IMP) provides an operational framework for the management of IT incidents that could have or have had an impact on the GC. Because the GC IT IMP deals with incidents related to either IT or ITS, an IT incident is understood to be:

- Any event that disrupts the normal operations of an organization and causes or may cause a reduction in the quality of service or in productivity; or
- Any unauthorized attempt, whether successful or not, to gain access to, modify, destroy, delete, or render unavailable any computer network or system resource.[1]

The objective of the GC IT IMP is to restore normal operations as quickly as possible and minimize the adverse effect on services to Canadians, government operations, and confidence in government. This ensures that the best possible levels of service, quality, and availability are maintained. [2]

To receive assistance in managing incidents, contact the
GOVERNMENT OPERATIONS CENTRE (GOC) at:
Email: GOC-COG@ps-sp.gc.ca
Telephone: 613-991-7000
Fax: 613-996-0995

1. Office of Critical Infrastructure Protection and Emergency Preparedness, Emergency and Crisis Communication Vocabulary, Terminology Bulletin 252.
2. Details of the ITIL v2 framework , http://en.wikipedia.org/wiki/ITIL#Incident_Management

Table of Contents

1. Introduction

The GC's security program and the continuity of GC operations rely upon the ability of departments[3] and government as a whole to manage actual or potential information technology (IT) incidents. All government departments experience events that either impact or threaten to impact government services and operations. The GC is increasingly dependent upon IT to deliver services to Canadians and maintain operations and must react quickly and effectively to any IT incident that may adversely affect services to Canadians, government operations, or confidence in government.

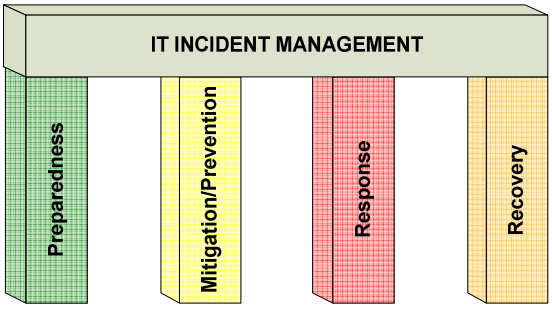

Figure 1: Four pillars of the IMP

The GC needs formal protocols and procedures to manage IT incidents and ensure GC-wide continuity of services and operations, especially as more and more of its service delivery capability and infrastructure is shared and integrated. In times of a threat to or disruption of services or operations, the GC must prioritize actions, mitigate impact, and minimize response times. Consequently, the GC IT IMP lays out the GC processes and identifies departmental roles and responsibilities for reporting actual and potential incidents and for responding when GC services and operations are interrupted or are otherwise affected by an IT incident. The GC IT IMP formalizes the cross-government reporting, warning, and response protocols to ensure that all relevant departments are appropriately engaged.

The *Government Security Policy* requires that departments establish mechanisms to respond effectively to IT incidents and exchange incident-related information with designated lead departments in a timely fashion. Strong horizontal coordination of incident management activities is critical to the successful resolution of incidents affecting the interests of the GC.

The GC IT IMP directly aligns with the widely accepted four pillars of emergency management—preparedness, mitigation/prevention, response, and recovery—and outlines activities for post-incident analysis so that lessons learned can be identified and applied. The GC IT IMP is an event-specific plan within the Federal Emergency Response Plan (FERP). The GC IT IMP framework, through its focus on the issues that have the greatest urgency and, potentially, the greatest impact on the GC, will ensure the effective and efficient management of IT incidents.

3. General use of departments in the plan includes agencies.

Objectives

- Improve GC situational awareness
- Ensure timely resolution of incidents that affect GC services, operations, and confidence in government
- Draw on and share GC knowledge and expertise
- Minimize the impact on Canadians, partners, and overall confidence in government
- Enhance the Canadian public's confidence in the GC's effectiveness
- Improve decisions, mitigation, and responses
- Improve coordination and incident management planning within the GC
- Instill a shared sense of responsibility among the GC IT and ITS communities

1.1 Authority

This Plan is prepared in support of the delegated authorities of the Minister of Public Safety under the *Emergency Management Act* as well as those delegated to the Treasury Board of Canada Secretariat under the *Financial Administration Act* and the associated *Government Security Policy*.[4]

1.2 Purpose

The purpose of this GC IT IMP is to provide an event-driven operational framework to integrate the federal response to IT threats, vulnerabilities, and incidents that impact or may impact the GC.

This GC IT IMP assembles IT incident management responsibilities from across the GC into a cohesive GC capability supported by individual departments, central agencies, lead agencies, and GC service providers[5] with relevant mandates.

The GC IT IMP:

- Establishes measures and processes to support its activation and execution;
- Establishes clear criteria and processes for its activation and execution, for reporting, and for response;

4. These mandate that Public Safety Canada advance federal preparedness (including response and recovery operations) for emergencies of all types, including those within the IT domain, and that the Treasury Board of Canada Secretariat monitors incidents that have an impact on government operations or that could require revisions to operation standards or technical documentation.
5. General use of GC service provider includes departments and agencies that provide common services to the GC.

- Identifies clear roles and responsibilities for horizontal direction, coordination, and communications;
- Identifies links with departmental IMPs; and
- Provides a flexible operational model that aligns with the Federal Emergency Response Plan (FERP) and facilitates the horizontal management of the GC response to IT incidents.

1.3 Scope

This Plan applies to all federal institutions subject to the *Government Security Policy* and addresses:

- Threats, vulnerabilities, and incidents within an IT environment that affect or may affect service to Canadians, government operations, or confidence in government; and
- Incidents within an IT environment requiring an integrated GC response (see section 1.8).

This Plan does not address:

- Departmental response to an IT incident, its handling or management, or other forms of business continuity planning activities because each department must align and coordinate its own internal IT incident management processes and continuity plans with the GC IT IMP;
- The coordination of national and international IT incidents, except where the incident affects services to Canadians, government operations, or confidence in government and triggers the need for a federal response; and
- Other forms of crisis and emergency management.

1.4 Assumptions

The following assumptions were made during the development of this Plan:

- If the incident is considered a crime, departments will report the incident directly to the Royal Canadian Mounted Police or local police authority;
- All departments within the GC will collaborate and contribute accordingly;
- Roles and responsibilities of departments will vary depending on the nature and scope of the incident;
- All organizations have incident management processes and plans and business continuity plans (BCP) in place as established under the *Government Security Policy*;
- All departments are familiar with the contents of the FERP;
- Current departmental mandates and responsibilities will be respected;
- IT incidents related to the disclosure of personal information follow established privacy procedures; and

- Departments classify, designate, communicate, and manage information according to the appropriate mechanisms. For further information, contact the departmental security officer.

1.5 GC IT Risk Environment

To date, a gap exists between how the state of GC-wide IT security is perceived and the development and communication of an integrated approach for maintaining and safeguarding its IT services. Existing data indicate that risk within the GC IT environment is ever evolving. Risks are increasing because attacks have clearer targets, are more complex, and require GC-wide coordination. In addition, Canadians are aware of the impact that IT threats and incidents can have on service delivery and, consequently, on their well-being.

Dependence on IT systems to support critical government operations continues to increase, along with the dependence on the Internet for the delivery of GC services to the Canadian public. IT systems are becoming increasingly complex yet remain vulnerable. Threat is constantly evolving in the increasingly interconnected, global environment, with attacks becoming more sophisticated and targeted.

Managing IT incidents within this global environment is a continuous challenge because of the constant barrage of new vulnerabilities, malicious code, and incidents. Besides susceptibility to the new or evolving threats brought on by this environment, system maintenance, power failures, natural disasters, and pandemics are also factors to be considered in contingency planning as they too could affect GC IT systems. Organizations must be continuously vigilant and ready to respond. Given the interdependency of GC departments and the overall impact a single incident can have on the confidence in government, no one single department can manage IT incidents in isolation.

Although the GC lacks adequate situational awareness information to fully assess the state of its IT security and the safeguards ensuring its continuity, recent incidents indicate that the GC is not immune to IT incidents and must be prepared. In addition, the GC is combatting criminal and national security threats. Because incidents that impact GC services are reported in the media, Canadians are made aware of the risk within the GC IT environment. Increasingly, incidents cannot be managed in isolation and require an integrated GC approach.

1.6 Objectives

Key objectives of the GC IT IMP include the following:

- Timely resolution of incidents to minimize impact on government services, operations, and confidence in government;

- Improved access to GC knowledge and expertise with regard to GC-wide incident management;
- Better understanding of the repercussions of IT incidents on the GC, allowing for improved prioritization to minimize the negative impacts on Canadians, partners, and overall confidence in government;
- Accurate information and status reports on actual or potential IT incidents to improve decision making, mitigation, and response;
- Improved coordination and IT incident management planning within the GC;
- Improved GC situational awareness to support an integrated outlook for the state of GC-wide IT security;
- Improved GC mitigating actions and preparedness activities for proactive prevention of and protection from IT incidents;
- Instill a shared sense of responsibility among the GC IT and ITS communities; and
- Enhanced public perception of the GC's effectiveness for responding to IT incidents that impact or could impact services to Canadians, government operations, or confidence in government.

1.7 Governance Model

During an incident, the timely engagement of senior government officials is key to a strong and effective proactive or reactive response. The governance model of the GC IT IMP identifies the senior management committees and officials who will be engaged when its trigger and severity criteria are met.

Figure 2 illustrates the direction and guidance the management committees will provide with respect to the four pillars of the GC IT IMP: preparedness, mitigation/prevention, response, and recovery. The engagement of the following committees and officials will be based on the circumstances and gravity of each situation:

- Management Team
- Federal Coordinating Officer
- Assistant Deputy Minister Emergency Management Committee
- Deputy Minister National Security Committee
- Cabinet Operations Committee

The roles and responsibilities of the committees are further detailed in Section 1.8.

Guidance provided by the committees and officials of the GC IT IMP governance structure will cover both short- and long-term activities. Short-term activities are event-driven and are carried

out during the mitigation of a threat or vulnerability or the response to or recovery from an incident. These activities require a quick and coordinated response, often within short time frames.

Longer-term activities involve post-incident analysis and lessons learned, preparedness, and mitigation, for which the Assistant Deputy Minister Security Committee (ADM Security) and the Chief Information Officer Council (CIOC) provide longer-term strategic leadership, direction, and governance related to security and IT respectively.

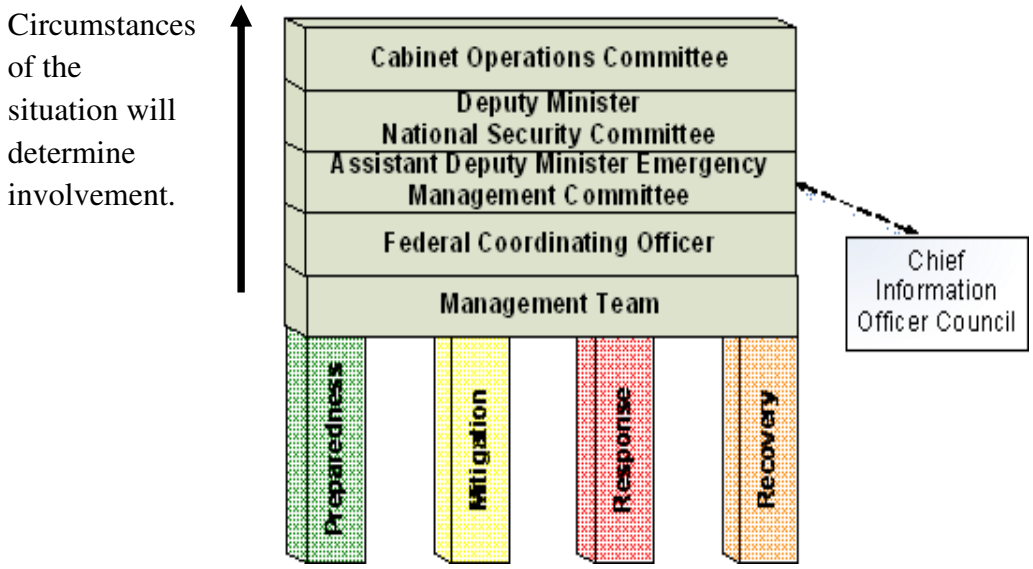

Figure 2: IMP Horizontal Governance

1.8 Roles and Responsibilities

To ensure the horizontal direction, coordination, and communication necessary for an integrated and cohesive federal response to IT incidents, Public Safety Canada (PS) will monitor incidents and potential threats around the clock and provide coordination and support. Figure 3 illustrates how horizontal direction, coordination, and communication are integrated.

Circumstances of the situation will determine involvement.

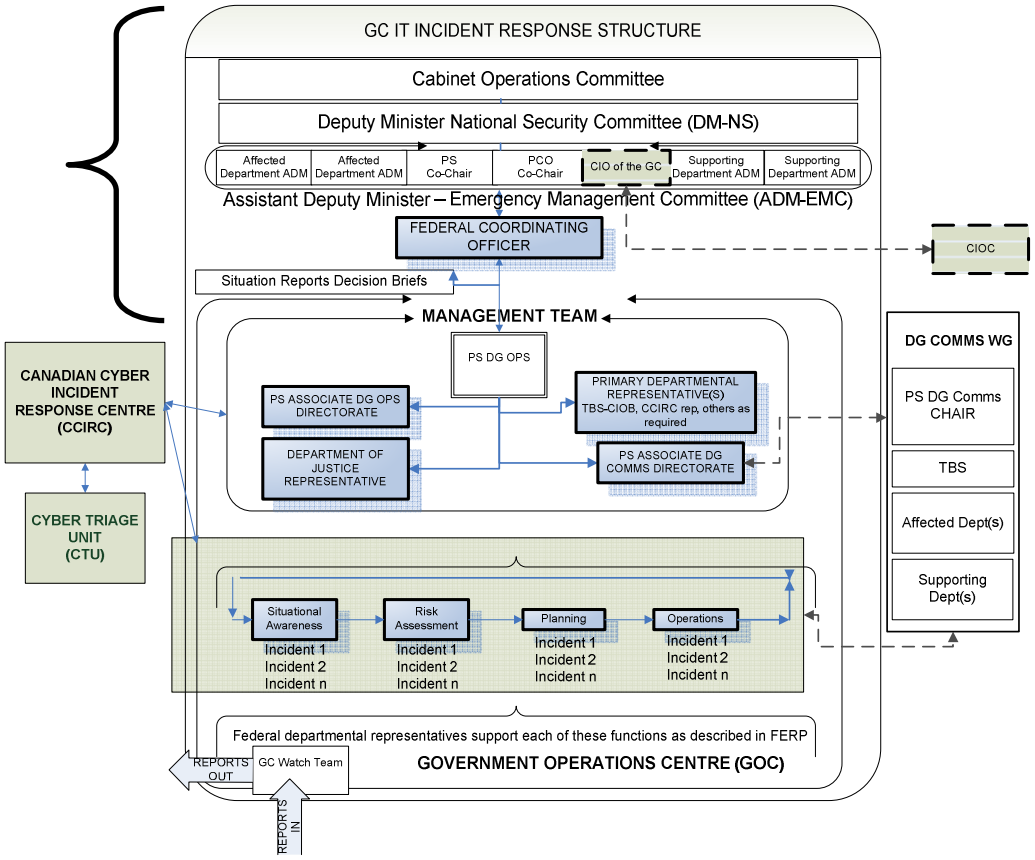

Figure 3: GC IT Incident Response Structure

1.8.1 Horizontal Direction

The GC IT IMP is aligned with the existing senior-level committee structure used under the FERP and also includes key officials and committees required to manage IT incidents that impact or may impact the GC. Escalation of a threat, vulnerability, or incident to these committees or officials will be done on an as-needed basis depending on the circumstances of the situation. Top-level senior management committees and officials include the following:

- The **Cabinet Operations Committee (Ops Committee)** oversees the GC response to an incident with a high impact on the GC[6] and will be engaged based on the direction of the Deputy Minister National Security Committee (DMNS). The Ops Committee provides direction to senior officials and may assign some or all of its responsibilities concerning the incident to the Cabinet Committee on Foreign Affairs and Security.

6. Appendix C: Impact Severity Assessment Matrix

*where operational constraints permit

- The **Deputy Minister National Security Committee (DMNS)** provides direction to the Assistant Deputy Minister Emergency Management Committee (ADM-EMC) and the Federal Coordinating Officer (FCO) during high-impact incidents[1] requiring an integrated GC response. DMNS will be engaged based on the direction of the ADM-EMC or the National Security Advisor. The DMNS is the primary committee responsible for coordinating the GC's response and for providing advice to ministers. Membership on this committee is based on the nature of the incident and can therefore be varied. The DMNS also determines the content of ministerial briefings and considers, recommends, and approves response actions for ministers.
- The **Assistant Deputy Minister Emergency Management Committee (ADM-EMC)** ensures lateral support across and within GC departments for the management of incidents. The ADM-EMC provides strategic direction and guidance to the FCO for medium- to high-impact incidents[1] (as determined by the FCO) and provides direction to officials within the GOC. The ADM-EMC will be engaged based on the direction of the Management Team or the FCO. The flow of information between the GOC and the ADM-EMC is illustrated in Figure 4. The ADM-EMC approves the content and substance of deputy minister briefings and recommends and coordinates options for response to the DMNS or the Ops Committee.

  Given the variable membership of this committee, its standing member for any IT incident that affects or may affect the operations or services of the GC or confidence in government is the Chief Information Officer for the Government of Canada.

- The **Chief Information Officer for the Government of Canada (CIO for the GC)** advises the ADM-EMC on incident-related issues, such as security and operations of GC IT systems and networks, service delivery, and confidence in government. The CIO for the GC is the chair of the broader community of CIOs in the GC and, through its CIO Council (CIOC), the conduit to that community. The CIO for the GC approves the following:
  - Disconnection of departmental infrastructures or systems if required to contain an incident and reduce its GC-wide impact, in consultation with the CIOC[*] and the affected department(s). This could include, but is not limited to, network interconnections, common or shared services, critical systems, and other departmental infrastructures.
  - Blocking or disconnection of limited services in cases where immediate containment action is required and the impact to government operations or critical services is minimal.
  - GC directive to apply mitigating safeguards as a pre-emptive action to reduce exposure to threats, vulnerabilities, or incidents and their possible effects.
- The **Chief Information Officer Council (CIOC)** is the advisory body to the CIO for the GC and will support the management of IT incidents that affect security, systems, networks,

service delivery, or confidence in government. The CIOC provides advice, direction, and guidance with respect to GC incident management, including, but not limited to, response and recovery plans.

- The **Federal Coordinating Officer (FCO)**, on behalf of the Minister of Public Safety, has the overall responsibility for the coordination of a federal response to an emergency.[7] Under the GC IT IMP, this includes any incident that meets its trigger and severity criteria. Either the Deputy Minister, PS or the Senior Assistant Deputy Minister, PS assumes the role of FCO.
- The **Management Team,** under the leadership of PS's Director General, Operations Directorate, manages the actions and functions of the Federal Emergency Response Management System (FERMS) and establishes and oversees the successful completion of the objectives set for each operational period.[8] In terms of the GC IT IMP, the Management Team is the executive-level team that provides strategic guidance to the GOC and the CCIRC when IT incidents meet the IMP's trigger and severity criteria. It is also the executive team that interfaces with the FCO and approves products for federal senior officials, such as decision briefs (see Appendix F). In addition to the Management Team representatives described in the FERP, the Management Team under the GC IT IMP also includes a departmental representative from the Treasury Board of Canada Secretariat's Chief Information Officer Branch (Secretariat CIOB) and, depending on the nature of the IT incident, from other primary departments.

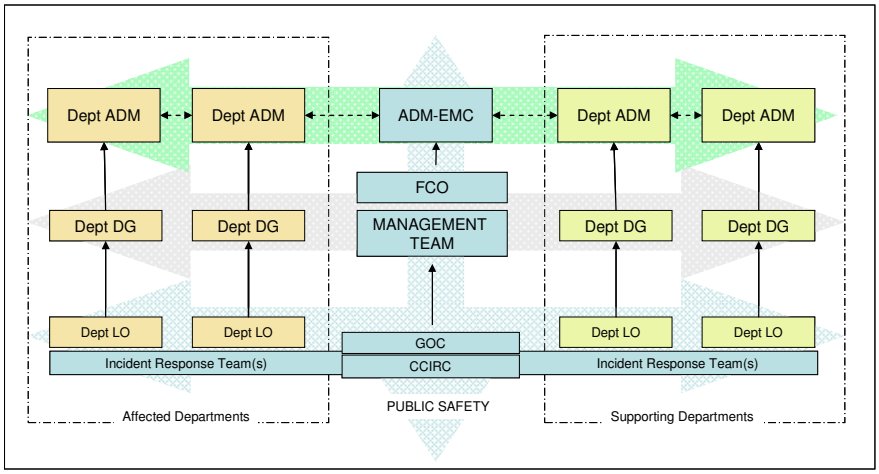

Figure 4 : Flow of Information between the GOC and the ADM-EMC

7. Federal Emergency Response Plan
8. Federal Emergency Response Plan

1.8.2 Coordination and Analysis

- The CCIRC is the central point for monitoring, and coordinating the response to, any IT incident in order to protect the GC.[9] The functions of the CCIRC are interfaced around the clock with the rest of the GC through the GOC. The CCIRC's mandate under the GC IT IMP requires support from and coordination among the following:
- The **Government Operations Centre (GOC)**, housed within PS on behalf of the GC, is the principal location where subject matter experts and liaison officers from government departments, non-governmental organizations, and the private sector (as appropriate) perform the primary functions of FERMS. Department-specific operations centres support their departmental roles and mandates and contribute to the integrated GC response through the GOC. The GOC, staffed during day-to-day operations by PS **watch officers,** is the interface between the CCIRC and the GC.
- Upon escalation to a FERP response level 2[10] or 3[11], departmental representatives may be called on to augment the GOC. This escalation depends on the circumstances of the situation and will occur when the Director General, Operations Directorate, in consultation with the Management Team and the FCO, deems an IT incident meets the IMP's trigger criteria (Section 1.9) and medium- or high-impact severity criteria. Depending on the circumstances of the IT incident, the GOC will call on subject matter experts or liaison officers from primary and supporting departments to support operations, situational awareness, risk assessment, and planning functions as outlined in the FERP. When the FERP is escalated, these departmental representatives will lend temporary support to the GOC and the Management Team, though their primary reporting responsibility remains to their respective departments.
- The **Canadian Cyber Incident Response Centre (CCIRC)** is the cyber coordination centre for the GC. The CCIRC receives incident reports from across the GC, from national and international partners, and from foreign governments.[12] The CCIRC analyzes this data against actual vulnerabilities and risks and augments its capabilities for analysis and response through the Cyber Triage Unit (CTU) and the GOC. To ensure strategic objectives are achieved, the CCIRC will—on a continuous and ongoing basis—inform the Secretariat CIOB of the status of incidents that meet the IMP's trigger criteria.

9. This is a subset of its expanded mandate, which includes the protection of national critical infrastructure.
10. FERP response level 2 refers to the partial augmentation of the GOC.
11. FERP response level 3 refers to extensive augmentation of the GOC.
12. The IMP recognizes the importance of analyzing information from various sources, therefore incident reports from partners outside the scope of the IMP are considered as direct input when assessing the potential or real impact on the GC.

- The **Cyber Triage Unit (CTU),** led by the CCIRC, works to ensure a rapid and focussed response to a cyber incident. The CTU is composed of officials from PS, the Royal Canadian Mounted Police, the Canadian Security Intelligence Service, National Defence,[13] and Communications Security Establishment Canada. The CTU is responsible for the following:
  - Analysis of incidents and warnings reported from federal, national, and international sources;
  - Assessment of the nature of an incident to identify a primary department and support roles; and
  - Exchange of information between departments.
- The **Primary Departments** are departments with a mandate related to a principle element of the incident. Certain representatives from these departments may be called upon by PS to fill various functions within the GOC, act as a liaison between PS and their respective departments, or communicate the incident response status to their department.
- The **Supporting Departments** are departments that provide general or specialized assistance to a primary department for responding to an incident. Certain representatives of these departments may be called upon by PS to fill various functions within the GOC, act as a liaison between PS and their respective departments, or communicate the incident response status to their department.
- The **Affected Departments** are departments that meet the IMP's trigger criteria and medium- or high-impact severity criteria (see Appendix C).

1.8.3 Communication

The GOC, which is housed within PS, is the interface between the GC and the CCIRC. Communications activities, including strategies and public communications, will be led by PS through:

- The **Public Safety Director General Communications (PS DG Communications)**—As established by the FERP, PS is the primary department responsible for the support function of communications during an emergency, coordinating and liaising with DGs of Communications from other departments.
- The **Director General Communications Working Group (DG Comms WG)**—Under the leadership of PS DG Communications, DG Comms WG brings together communications representatives from the Secretariat and Affected and Supporting Departments (where applicable) to coordinate the communications aspects of the incident.

13. National Defence is a proposed member of the CTU (currently under discussion).

1.8.4 Continuity and Oversight

Ongoing support and management functions for the GC IT IMP will be performed by the following:

- The **Secretariat CIOB** will be responsible for oversight of the GC IT IMP. To fulfill this oversight role and to ensure that the strategic objectives of the GC are maintained, the CCIRC will inform, on a continuous and ongoing basis, the Secretariat CIOB of incidents meeting the IMP's trigger and severity criteria. In addition, the Secretariat CIOB will receive all post-incident action plans and, when warranted, perform post-mortems on incident activities, track the status of post-incident action reports, develop and maintain a repository for GC lessons learned, and develop, maintain, and make adjustments, where required, to policy instruments and the GC IT IMP.
- The **CIOC,** as the advisory body to the CIO for the GC, will provide advice and guidance with respect to GC incident management. In addition, the CIOC will provide strategic direction and leadership with regard to preparedness, mitigation, and post-incident analysis activities. The CIOC will receive periodic summary reports on IT incidents affecting the GC.
- The **Assistant Deputy Minister Security Committee (ADM Security)**, as an advisory body for security within the GC during normal operations, will provide strategic governance and advice, including strategic actions identified in post-incident analysis and follow-up. In addition, ADM Security will provide strategic direction and leadership with regard to preparedness, mitigation, and post-incident analysis activities related to security and will receive periodic summary reports on IT incidents affecting the GC.

1.9 Implementation—Trigger Criteria

While preparedness against threats, vulnerabilities, and incidents under the GC IT IMP is the responsibility of every GC department, their severity could trigger escalation to the federal level. Any one of the following, or a combination thereof, will prompt escalation:

- The threat, vulnerability, or incident affects critical departmental services or infrastructures, as identified in departmental BCPs;
- The threat, vulnerability, or incident requires an integrated GC response because:
  - there is a cross-cutting effect whereby a threat, a vulnerability, or an incident affecting one department has or could have a potential negative impact or unknown impact on other departments;
  - the threat, vulnerability, or incident could affect more than one department; or
  - there is a high probability that common services will be affected;

- The threat, vulnerability, or incident affects other jurisdictions, significant partners, or critical infrastructure sectors where a single point of entry into the GC is required;
- The threat, vulnerability, or incident affects employees, delivery of services to Canadians, or confidence in the GC; and
- The threat, vulnerability, or incident has an impact on national security or the privacy of Canadians through unauthorized disclosure of electronically held, stored, processed, or transmitted sensitive information.[14]

Note: If uncertainty exists, departments should contact the CCIRC for assistance in characterizing the threat, vulnerability, or incident further and clarifying incident reporting requirements. The CCIRC will engage the cyber specialists of the CTU to assess the nature of the incident and its potential impact and institute GC-wide protective measures.

Trigger Criteria

Will or could the IT threat, vulnerability, or incident:

- Impact critical departmental services or infrastructures?
- Have a cross-cutting impact whereby the impact on one department has or could have an effect on other departments?
- Affect more than one department?
- Affect common services?
- Impact employees, service delivery to Canadians, or confidence in the GC?
- Affect national security or have an impact on the privacy of Canadians through unauthorized disclosure of electronically held, processed, transmitted, or stored sensitive information?
- Impact other jurisdictions, significant partners, or critical infrastructure sectors where a single point of entry into the GC is required?

14. In accordance with SPIN 2008-02 Reporting IT Incidents

2. Concept of operations

The GC IT IMP provides a comprehensive approach for managing threats, vulnerabilities, and incidents. While respecting the authority of each deputy head, the GC as a whole must consider the broader impacts that threats, vulnerabilities, and incidents have or may have on services to Canadians, government operations, or confidence in the GC. That said, departments will continue to safeguard IT operations and availability and ensure that appropriate incident response mechanisms are in place to support all phases of incident management while, at the same time, respecting the integrated approach of the GC IT IMP.

2.1 Operational Model

To successfully meet the objectives of the GC IT IMP, departments and the GC will support and contribute to the following components of its operational model (see Figure 5):

- the set of broad continuous processes within preparedness;
- the pre-emptive actions within mitigation;
- the reactive activities within response; and
- the return to normal operations within recovery.

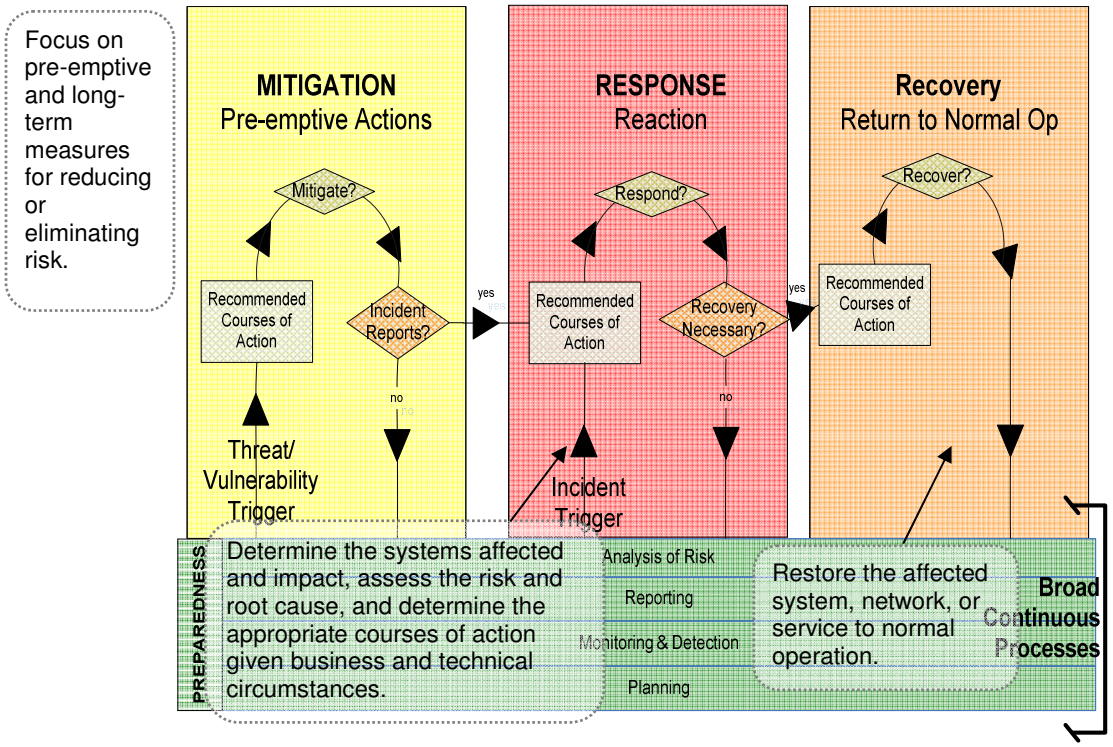

Figure 5: GC IT IMP Operational Model

Preparedness is the foundation of the operation model and involves the set of broad continuous processes that are part of normal operations in an IT environment: planning, monitoring, analyzing risk, and reporting. These processes prepare for specific or unpredictable events or situations and identify those threats, vulnerabilities, or incidents that trigger GC-wide actions of mitigation, response, or recovery. The processes within preparedness are ongoing. For example, monitoring activities continue throughout mitigation, response, and recovery phases. Similarly, longer range strategic activities within planning typically take into account trends found among incidents or other environmental changes that impact risks and require mitigating action.

Mitigation includes pre-emptive actions that are taken to prevent vulnerabilities and threats from becoming incidents or to reduce the effects of incidents when they occur. The mitigation phase differs from the other phases because its measures focus on reducing or eliminating risk in a proactive fashion rather than the reactive measures of response and recovery. Ideally, mitigation activities are triggered early enough to allow long-term protective measures to be taken. Threats and vulnerabilities will be elevated to a GC-level response by departments, the CCIRC, or the CTU when the IMP's trigger criteria are met.

Response is the mobilization stage where the appropriate courses of action are determined to safeguard services that have been or may be affected by the incident. Incidents will be elevated to a GC-level response when a threat, vulnerability, or incident meets one or more of the IMP's trigger criteria. The primary objective of this phase is to contain the incident quickly and analyze its root cause. Additional analysis will be carried over into the recovery phase.

Recovery restores the affected system, network, or service to normal operations. In some instances, essential services may be temporarily restored to a degraded state as defined in BCPs. This phase is concerned with issues to be addressed and decisions to be made after the immediate threat of the incident has subsided and the incident is contained.

2.2 Preparedness Phase

Purpose

As part of normal operations, preparedness is an ongoing phase where a set of broad continuous processes ready the GC for specific or unpredictable events or situations and identify those threats, vulnerabilities, or incidents that trigger GC-wide actions of mitigation, response or recovery.

Activities

Planning describes how personnel, equipment, and other resources are used to support incident management activities. The GC's plans provide mechanisms and systems for setting priorities, integrating multiple organizations and functions, and ensuring that communications and other capabilities are available and integrated to support a full spectrum

of incident management requirements. Departmental and GC service provider plans must work in conjunction with the GC-wide plan when an IMP criterion is triggered. In addition, incident management plans must be reflected (where applicable) in service level agreements (SLA).

Monitoring and Detection are performed to identify changes in the operational environment that impact or could potentially impact service to Canadians, government operations, or confidence in government. Events that are early indicators of future incidents, such as emerging threats and vulnerabilities, could be revealed through monitoring and detection.

Reporting ensures the timely communication of emerging IT threats, vulnerabilities, and incidents that impact or could potentially impact GC services, operations, or confidence in government. Departments must report anomalies or events that are or may be indicators of an incident that meets the IMP's trigger criteria.

Analysis of Risk utilizes departmental reports sent to the CCIRC when a department's analysis results in triggering the IMP criteria. The CCIRC will share this departmental report with the CTU to perform a GC-wide analysis of risk (including impact and likelihood). This information will be provided to the senior management committees for review and approval of the GC-wide course(s) of action.

2.2.1 Planning

Purpose

Planning describes how personnel, equipment, and other resources are used to support incident management activities and lays the groundwork for ensuring those plans can be activated. The GC's plans provide mechanisms and systems for setting priorities, integrating multiple entities and functions, and ensuring that communications and other capabilities are available and integrated to support a full spectrum of incident management requirements. Departmental plans must integrate and work in conjunction with the GC-wide plans when an IMP criterion is triggered. In addition, incident management plans must be reflected (where applicable) in SLAs.

Activities

Identifying and understanding critical systems is fundamental to the support of incident management activities. Without understanding what is most critical to the GC, the assessment of risk would lack the ability to characterize the impact. To identify critical systems, business requirements, such as information and services, must be understood in light of a system's strengths and weaknesses—that is, understanding the safeguards in place, the vulnerabilities of the system, and the related exploits known within the public domain.

2.2.1.1 Identifying

2.2.1.1.1 **Departments will** identify their critical systems.

2.2.1.1.2 **PS will** identify GC critical systems based on that departmental identification and inventory.

2.2.1.1.3 The **Secretariat will** lead and engage strategic senior management committees to ensure planning and preparedness issues within the GC are identified and addressed.

2.2.1.2 Developing

The policy instruments developed (including plans) need to support incident management activities and clearly identify roles and responsibilities. Establishing plans, expectations, and rules of engagement for the key players prior to, during, and after an IT threat, vulnerability, or incident is essential.

2.2.1.2.1 **Departments will** integrate the processes of the GC IT IMP into their departmental IT plans.

2.2.1.2.2 **PS will** develop and maintain standard operating procedures for the IMP's various components (e.g. communications, GOC, and CCIRC).

2.2.1.2.3 The **Secretariat will** develop and maintain the GC IT IMP.

2.2.1.2.4 The **Secretariat will** incorporate lessons learned from previous incidents, mitigation strategies, exercises, and tests into GC policy instruments.

2.2.1.2.5 The **Secretariat will** promote best practices and ensure the implementation of the GC Lessons Learned Action Plan.

2.2.1.3 Training

Key players and departments must be educated and trained on the GC IT IMP's processes, organizational structure, and operating procedures in order to react effectively and efficiently in the face of a potential or actual threat, vulnerability, or incident. This includes clearly understanding roles, responsibilities, and expectations, which, through interdepartmental exercises and scenarios, will improve integration and interoperability and optimize how resources are used during incident management.

2.2.1.3.1 **Departments will** participate in GC IT IMP training.

2.2.1.3.2 The **Secretariat will** ensure that training sessions for departmental IMP representatives are developed.

2.2.1.4 Testing

GC incident management activities must be tested in realistic, multidisciplinary, and interdepartmental exercises and scenarios to improve integration and interoperability and optimize how resources are used during incident operations.

2.2.1.4.1 **Departments will** participate in GC IT IMP exercises, scenarios, and tests.

2.2.1.4.2 **PS will** test the GC IT IMP using realistic exercises and scenarios to validate its effectiveness and identify gaps.

2.2.1.4.3 The **Secretariat will** ensure testing of the GC IT IMP and implementation of resulting lessons learned.

Inputs	Outputs
• Information on lessons learned from previous incidents, mitigation strategies, exercise, and test scenarios • Mitigation strategies • Best practices	• GC inventory of critical services and associated IT dependencies and defenses • GC-wide incident management mitigation strategies, policies, plans, and processes • Training sessions for departmental IMP representatives • Exercises, scenarios, and tests that validate the efficiency and efficacy of both the GC IT IMP and departmental plans • Departmental IMPs that integrate the GC IT IMP • Best practices

2.2.2 Monitoring & Detection

Purpose

Monitoring and detection involves continuously watching for and recognizing events or early indications of an emerging threat, vulnerability, or incident and assessing the validity and impact of a security incident or IT outage on service to Canadians, government operations, or confidence in government.

Activities

The continuous monitoring (and analysis) of threats, vulnerabilities, and indicators of potential incidents at the departmental and GC-wide levels is necessary to identify possible or actual adverse effects on GC infrastructure. Detection occurs as a direct result of monitoring. If the monitoring component is inadequate or incomplete, the detection process will most likely miss certain anomalies or events that could indicate an actual or potential threat, vulnerability, or incident. Under the *Government Security Policy*, departments must continuously monitor the operations of their systems to detect anomalies or events that would lead to or that indicate a high potential for the occurrence of an incident. Without monitoring, the detection of anomalies or events that are or may be indications of an incident would be next to impossible. The detection of a threat, a vulnerability, or an incident within one department could provide advance notification of a serious security breach or IT outage that could adversely affect other departments, services to Canadians, government operations, confidence in government, or the GC as a whole.

2.2.2.1 Monitoring and Analysis

2.2.2.1.1 **Departments will** carry out the monitoring and detection activities as established under the *Government Security Policy* (e.g. track and analyze threats, vulnerabilities, events, and incidents that may affect departmental IT systems).

2.2.2.1.2 **Departments will** contact the CCIRC for assistance if uncertain of the characterization of an event, threat, vulnerability, or incident.

2.2.2.1.3 **Departments will** monitor information from the CCIRC (e.g. GC status reports, requests for information—RFI, GC incident reports, GC incident situation reports, warnings, and GC situational awareness reports) and respond accordingly.

2.2.2.1.4 The **CTU will** monitor the GC environment in conjunction with its members (listed below) and in accordance with their respective mandates regarding actual or potential threats, vulnerabilities, or incidents:

2.2.2.1.4.1 **The** Royal Canadian Mounted Police will **monitor criminal surveillance sources;**

2.2.2.1.4.2 **The** Canadian Security Intelligence Service will **monitor intelligence surveillance sources;**

2.2.2.1.4.3 Communications Security Establishment Canada will **monitor technological IT threats and provide technical threat and incident analysis and mitigation advice;**

2.2.2.1.4.4 Communications Security Establishment Canada will **collect and provide primary source foreign Signals Intelligence (SIGINT) reporting regarding cyber threats;**

2.2.2.1.4.5 National Defence will **monitor information from allied sources, including NATO; and**

2.2.2.1.4.6 National Defence will **monitor technological IT threats.**

2.2.2.1.5 Members of the **CTU will** work with the CCIRC to assess whether an emerging threat, vulnerability, or incident, as measured against the IMP's trigger and impact severity criteria, could affect the GC's critical assets or the availability of its services.

2.2.2.2 Coordination and Analysis

2.2.2.2.1 To detect an actual or a potential threat, vulnerability, or incident, the **CCIRC will** monitor and analyze technical sources and the information reported by:

2.2.2.2.1.1 GC departments

2.2.2.2.1.2 CTU members

2.2.2.2.1.3 Open sources

2.2.2.2.1.4 National and international partners[15]

2.2.2.2.2 The **CCIRC will** consult with the CTU to assess whether an emerging threat or vulnerability could result in an incident that meets the IMP's trigger and impact severity criteria.

15 Although the interaction and processes between the CCIRC and national and international partners is out of the scope of the IMP, the information that is reported and shared with the CCIRC will be analyzed against the IMP's trigger and impact severity criteria.

2.2.2.2.3 The **CCIRC will** issue an RFI to departments to identify the threat across the GC landscape and determine if other departments are having similar indications of a threat, a vulnerability, or an incident.

2.2.2.2.4 The **CCIRC will** respond to departmental requests for specific technical advice, guidance, and information on IT incident detection.

Inputs	Outputs
• Open source • Reports of incidents and threats affecting the GC's critical assets and availability of its services • Reports of incidents suspected of constituting criminal offences • Reports of incidents involving threats to national interests • Information products from the CCIRC, by way of the GOC • Initial incident reports from departments to the CCIRC	• Identification of new or potential threats, vulnerabilities, or incidents that require GC-wide action

2.2.3 Reporting

Purpose

Timely reporting of emerging IT threats, vulnerabilities, events, and incidents affecting or potentially affecting GC services, operations, or confidence in government is vital.

Activities

2.2.3.1 Reporting

2.2.3.1.1 **Departments will** report an emerging IT threat, vulnerability, or incident that meets the IMP's trigger criteria to the CCIRC, by way of the GOC, as soon as it has been detected.

GOVERNMENT OPERATIONS CENTRE (GOC)

Email: GOC-COG@ps-sp.gc.ca
Telephone: 613-991-7000
Fax: 613-996-0995
Secure fax: 613-991-7094

Departments will send an initial departmental incident report to the CCIRC, by way of the GOC, when an IMP trigger criterion is met. The incident report will include the following:

2.2.3.1.1.1 Reporting department's contact information for follow-up;

2.2.3.1.1.2 Description of the incident, including time and location;

2.2.3.1.1.3 Estimated impact based on criterion triggered; and

2.2.3.1.1.4 Status of mitigating actions and an indication if assistance is required.

2.2.3.1.2 **Departments will** contact the CCIRC for assistance in characterizing the event if uncertain whether the event is a threat, vulnerability, or incident and also for clarification on incident reporting requirements.

2.2.3.1.3 **Departments will** send, when further information becomes available, an updated departmental incident report to the CCIRC, by way of the GOC (see Appendix D).

2.2.3.1.4 Members of the **CTU will** report to the CCIRC with information—from their respective areas of expertise—related to an actual or potential emerging threat, vulnerability, or incident affecting or potentially affecting services to Canadians, government operations, or confidence in government (see 2.2.2.1.4).

2.2.3.2 Reporting and Coordination

2.2.3.2.1 The **CCIRC will** function as the central point for departmental reporting of real or potential emerging threats, vulnerabilities, or incidents that affect or could affect services to Canadians, government operations, or confidence in government

2.2.3.2.2 The **CCIRC will** perform an initial analysis of the reported information against the IMP's trigger criteria. Reports can originate from the following:

2.2.3.2.2.1 External sources—any national, international, or allied partner of Canada;

2.2.3.2.2.2 Departments—any department within the GC;

2.2.3.2.2.3 CTU members—through analysis of information from sources within each member's departmental mandate; and

2.2.3.2.2.4 CCIRC—through situational awareness and analysis of information from various sources.

2.2.3.2.3 Where applicable, the **CCIRC will** send a confirmation receipt to all departments that have reported an incident to ensure they are aware the incident is being analyzed and triaged across the GC.

2.2.3.2.4 The **CCIRC will** issue electronic information products (cyber flashes, alerts, advisories, technical briefs, and other direction, information, or advice related to the threats, vulnerabilities, or incidents) to departments. Figure 6 illustrates the flow of information between the CCIRC (by way of the GOC) and Affected Departments. The following electronic information products will be shared with all departments unless the circumstances surrounding an incident warrant otherwise:

2.2.3.2.4.1 *Alerts* are extremely time sensitive products that describe an immediate or active security issue.

2.2.3.2.4.2 *Advisories* are not as urgent as alerts but still describe security threats and issues that could affect the state of the GC's IT security. Advisories also contain mitigation advice.

2.2.3.2.4.3 *Cyber flashes* are similar in urgency and content to advisories, yet they contain no official mitigation advice to address the vulnerability. Cyber flashes, unlike both alerts and advisories, are not publicly posted.

2.2.3.2.4.4 *Updates* are used to complement, correct, or update any of the electronic information products issued by the CCIRC. Updates ensure the GC has all available information.

2.2.3.2.4.5 *Situation reports* are sent out by the GOC to provide current information pertaining to the incident and the immediate and future response actions (see Appendix E). The report also identifies issues to be addressed and includes an analysis of the incident's impact on the GC. Typically, a situation report is issued for every

operational period or as directed by the Director General, Operations Directorate.

2.2.3.2.5 **Departments will** respond to the CCIRC's electronic information products as requested.

2.2.3.2.6 The **CCIRC will** respond to requests from departments for specific technical advice, guidance, and information on IT incident reporting.

2.2.3.2.7 The **CCIRC will** confirm the existence of a GC-wide incident and notify the Management Team.

2.2.3.2.8 The **CCIRC will** report to the Secretariat CIOB on statistics, trends, and emerging issues and incidents.

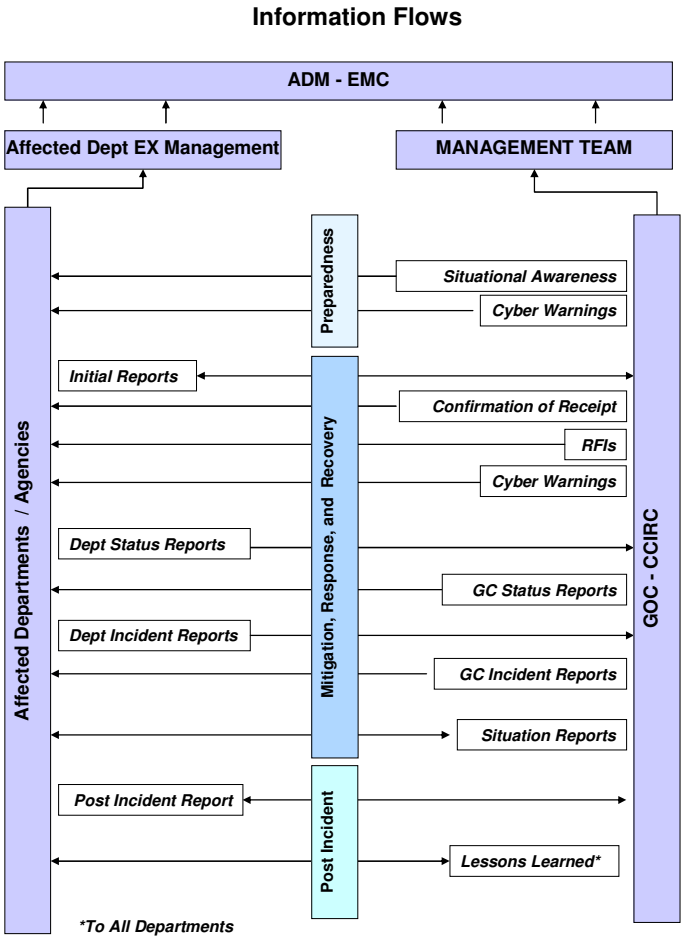

Figure 6: Flow of Information between the CCIRC (by way of the GOC) and Affected Departments

Inputs	Outputs
• Information products from the CCIRC, by way of the GOC • Initial incident reports from departments to the CCIRC • Reports from members of the CTU to the CCIRC	• Reports of incidents and threats affecting the GC's critical assets and availability of its services • Reports of incidents suspected of constituting criminal offences • Reports of incidents involving threats to national interests • Notification of the Management Team of an incident that triggered the response phase of the GC IT IMP

2.2.4 Analysis of Risk

Purpose

Analysis of risk is a continual process that will directly support the mitigation, response, and recovery phases of the GC IT IMP. Analysis of risk ensures that suspicious events or emerging threats, vulnerabilities, or incidents are analyzed from a GC-wide perspective utilizing up-to-date assessments and, where applicable, departmental assessments. This may include assessments from external sources coming into the CCIRC (see 2.2.3.2.2).

Activities

2.2.4.1 Continual Analysis

2.2.4.1.1 **Departments** will perform analysis of risk on their respective systems and business operations for threats, vulnerabilities, and incidents that meet the IMP's trigger criteria and share this with the CCIRC, by way of the GOC.

2.2.4.1.2 Members of the **CTU will** continuously share analysis information with the CCIRC to ensure coordination and a comprehensive perspective on the GC landscape (see 2.2.3.14).

2.2.4.1.3 The **CCIRC will** share the departmental risk analysis with the CTU.

2.2.4.1.4 The **CTU will** perform a broader, GC-wide analysis of the incident's potential or actual impact.

2.2.4.1.5 The **CCIRC will** assess all information received from various sources on a continuous basis and, where applicable, identify trends or potential areas of concern that meet or could meet the IMP's trigger criteria.

2.2.4.1.6 If the CCIRC's analysis identifies a potential or actual threat, vulnerability, or incident, it will trigger mitigating or response actions (see 2.3.1 and 2.4.1 respectively) depending on the circumstances of the situation.

Inputs	Outputs
• Information resulting from departmental assessments of risk • Information resulting from the CTU's assessments of risk	• A broad, GC-wide perspective on the risk environment • Indications of incidents and threats potentially affecting the GC's critical assets and availability of its services • Indications of incidents suspected of constituting criminal offences • Indications of incidents potentially involving threats to national interests • Information on threats, risks, and mitigating measures • Assessment of the nature and scope of the emerging threat, vulnerability, or incident against the IMP's trigger criteria

2.3 Mitigation

Purpose

Mitigation can either prevent vulnerabilities and threats from becoming incidents or reduce the effects of incidents when they occur. The mitigation phase differs from the other phases because its measures focus on reducing or eliminating risk in a proactive fashion rather than the reactive measures of response and recovery. Ideally, mitigating actions are triggered early enough to allow for long-term protective measures to be taken. Threats and vulnerabilities will be raised to a GC-level response by departments, the CCIRC, or the CTU when the IMP's trigger criteria are met.

Activities

2.3.1 Mitigation Activation

2.3.1.1 The mitigation phase is activated when the CCIRC receives a report from a department (or other sources as outlined in 2.2.3.2.2) of a vulnerability of threat that meets the IMP's trigger criteria (Section 1.9). Reports are submitted to the CCIRC through the GOC. The **CCIRC will** perform an initial analysis of the report's information against the trigger criteria.

2.3.2 Notification of the Management Team

2.3.2.1 As soon as it is confirmed that a vulnerability or threat has met the trigger criteria or when the CTU has been activated, the **CCIRC will** notify the Management Team of the information at hand.

2.3.2.2 The **head of the Management Team (PS's Director General, Operations Directorate) will** notify the following members of the Management Team:

2.3.2.2.1 PS's Associate Director General, Operations Directorate

2.3.2.2.2 Department of Justice Canada representative

2.3.2.2.3 PS DG Communications (for activation of the communications cycle)

2.3.2.2.4 Representatives of the Primary Departments:

2.3.2.2.4.1 Secretariat CIOB

2.3.2.2.4.2 Director of the CCIRC

2.3.2.2.4.3 Others as determined by the Director General, Operations Directorate, depending on the circumstances of the situation

2.3.3 Situational Awareness

2.3.3.1 Information regarding the threat or vulnerability is validated against the IMP's trigger criteria and the **CCIRC will:**

2.3.3.2 Activate the CTU according to its standard operating procedures (if activated, the analysis described in 2.3.3.4 would be done in consultation and coordination with the CTU).

2.3.3.2.1 The **CTU will** conduct focussed analysis on the circumstances of the situation (further to 2.2.4.1.4).

2.3.3.2.2 The **CTU will** identify Primary and Supporting Departments and make a recommendation to the Management Team as to the key players in the mitigation of the threat or vulnerability.

2.3.3.2.3 The **Royal Canadian Mounted Police will** proceed with a criminal investigation, concurrent with the GC response.

2.3.3.2.4 **National Defence will** proceed with a military options analysis and response, concurrent with the GC response, when there is a threat to its systems and those of the Canadian Forces or there is a cyber threat from any foreign military.

2.3.3.2.5 The **Canadian Security Intelligence Service will** proceed with an investigation, concurrent with the GC response, when there is a question of national security or a significant event.

2.3.3.2.6 **Communications Security Establishment Canada will**, concurrent with the GC response, monitor technological IT threats, provide technical threat and incident analysis and mitigation advice, and support investigations.

2.3.3.3 Engage Affected, Primary, and Supporting Departments to assist with analysis.

2.3.3.4 Analyze the threat or vulnerability to identify the systems affected, the users affected, and the impact on business by:

2.3.3.4.1 Identifying the root cause of the threat or vulnerability;

2.3.3.4.2 Analyzing the ongoing and potential impact on the GC's critical services, assets, and infrastructure based on the Impact Severity Matrix (see Appendix C);

2.3.3.4.3 Assessing the likelihood of an incident occurring based on the available intelligence and threat assessments;

2.3.3.4.4 Prioritizing actions in the event that multiple threats or vulnerabilities exist; and

2.3.3.4.5 Developing potential courses of action, each with its associated risks, anticipated level of effort, and timelines, to mitigate the threat or vulnerability.

2.3.3.5 The **CCIRC will** work with a communications liaison (as needed).

2.3.3.6 The **CCIRC will** recommend the most appropriate courses of action to the Management Team for review and approval.

2.3.4 Decision Points for the Mitigation Course of Action

2.3.4.1 The **Management Team will** be the first level of executive management to direct the actions necessary to mitigate the threat or vulnerability facing the GC.

2.3.4.2 The **Management Team will** approve a recommended course of action from those proposed by the CCIRC based on risk tolerance and the current GC environment.

2.3.4.3 The **Management Team will** determine the communications plan. PS DG Communications will coordinate, direct, and lead the communications effort accordingly, potentially engaging the DG Comms WG.

2.3.4.4 Depending on the circumstances of the situation, the **Management Team may** decide to escalate the situation in the following manner:

2.3.4.4.1 Escalation to FERP response level 2 or 3 response, depending on the likelihood, severity, and scope of mitigating actions; and

2.3.4.4.2 Escalation to the executive committees, which include the following:

2.3.4.4.2.1 FCO,

2.3.4.4.2.2 ADM-EMC,

2.3.4.4.2.3 DMNS, and

2.3.4.4.2.4 Ops Committee.

2.3.4.5 The **Management Team will** approve decision briefs (where appropriate) and situation reports prepared by the GOC to advise the executive committees of the potential impact on service to Canadians, government operations, or confidence in government.

2.3.4.6 The **Management Team will** choose a course of action from those proposed by the CCIRC (see 2.3.3.6) and set its direction. This will result in the approval of the GC mitigation plan, which is determined either by the Management Team or in consultation with the executive committees.

2.3.4.7 The **Management Team will** direct the CCIRC, by way of the GOC, to coordinate the implementation of the GC-wide mitigation plan. This may include, but is not limited to, notification of departments on specific mitigating measures and the requirement to report back to the CCIRC, by way of the GOC, with a status report or situation report.

2.3.5 Implementation of the GC Mitigation Plan

2.3.5.1 As directed by the Management Team, the **CCIRC will** coordinate, by way of the GOC, the implementation of the GC-wide mitigation plan and work with departments

(accordingly) to ensure awareness of the situation at hand and preparedness to deploy mitigating measures as required.

2.3.5.2 Where applicable, the **CCIRC will** advise, by way of the GOC, departments of specific mitigating measures and any requirements to report back to the CCIRC, by way of the GOC, with a status report or situation report.

2.3.5.3 **Affected Departments** (and where applicable all departments) **will** work to implement any relevant GC mitigating measures within their respective department.

2.3.5.4 Where applicable, **departments will** report back to the CCIRC, by way of the GOC (see 2.2.3.2.5).

2.3.5.5 The **CCIRC will** assess the residual risk utilizing the departmental situation reports and advise the Management Team of the risk, the situation, or changes in either based on this assessment.

2.3.5.6 The **CCIRC will** conduct ongoing situation and risk analysis to determine if the scope of the threat or vulnerability is mitigated within the identified Affected Departments and will report its findings to the Management Team.

2.3.5.6.1 In the mitigation status and situation report to the Management Team, the **CCIRC will** advise if the threat or vulnerability has been successfully mitigated. The **CCIRC will** also identify any related incidents that meet the IMP's trigger criteria and advise the Management Team to activate the response phase (see 2.4.2).

2.3.6 Decision Points—Confirmation of Mitigation

2.3.6.1 **The Management Team will** review the mitigation status and situation report from the CCIRC and, where applicable, consult further with the Affected Departments.

2.3.6.2 **The Management Team will** brief the executive committees accordingly, depending on which, or if any, of the executive committees were engaged (see 2.3.4.4.2). The executive committees that were engaged will provide further direction.

2.3.6.3 The **Management Team will** decide whether or not to close the mitigation stream or continue to monitor for specific or related threats or vulnerabilities.

2.3.6.3.1 If the decision is to continue to monitor for specific threats or vulnerabilities, any additional information will be validated and analyzed (see 2.3.3.1).

2.3.6.3.2 If the Management Team decides to close the stream, then post-incident analysis (see 2.6) will be conducted, concurrent with a return to the set of broad continuous processes of preparedness.

Inputs	Outputs
• Departmental and situation reports • Intelligence information (where applicable) • Criminal surveillance information (where applicable) • Significant event information (where applicable) • Publicly known vulnerabilities and threats • System logs (where applicable) • GC critical systems and services inventory • Technical resources • Political considerations • Legal considerations • Business objectives	• Detailed analysis of the threat or vulnerability • Situational awareness reports (bidirectional from departments to the CCIRC and from the CCIRC to departments) • Notification of executive management and committees of the GC IT IMP • Engagement of representatives from Primary, Supporting, and Affected Departments • Approved GC mitigation plan • Mitigation to the threat or vulnerability • Information products • Communications products • Where applicable, validated eradication of the threat or vulnerability

2.4 Response

Purpose

During the response phase, appropriate actions, activities, and services are mobilized when the impact from an incident meets one or more of the IMP's trigger criteria. The immediate objective of this phase is to contain the incident quickly and analyze the root cause. Depending on the extent of the damage, additional analysis may be carried over into the recovery phase.

Activities

2.4.1 Response Activation

2.4.1.1 The response phase is activated when the CCIRC receives reports of actual or potential incidents from departments (or other sources as outlined in 2.2.3.2.2) that meet the IMP's trigger criteria (Section 1.9). The **CCIRC will** perform an initial analysis of the information against the trigger criteria.

2.4.1.2 If the trigger criteria are not met, the **horizontal GC coordination (CCIRC) will** return to the preparedness phase.

2.4.2 Notification of the Management Team

2.4.2.1 As soon as it is confirmed that an incident has met the trigger criteria or when the CTU has been activated, the **CCIRC will** notify, by way of the GOC, the Management Team of the information at hand.

2.4.2.2 The **head of the Management Team** (PS's Director General, Operations Directorate) **will** notify the following members of the Management Team:

2.4.2.2.1 PS's Associate Director General, Operations Directorate

2.4.2.2.2 Department of Justice Canada representative

2.4.2.2.3 PS DG Communications (for activation of the communications cycle)

2.4.2.2.4 Representatives of the Primary Departments:

2.4.2.2.4.1 Secretariat CIOB

2.4.2.2.4.2 Director of the CCIRC

2.4.2.2.4.3 Others as determined by the Director General, Operations Directorate, depending on the circumstances of the situation

2.4.3 Situational Awareness

2.4.3.1 Using the information from incident reports and the set of broad continuous processes of the preparedness phase, the **CCIRC will**:

2.4.3.2 Validate the incident report against the IMP's trigger criteria; and

2.4.3.3 Activate the CTU according to its standard operating procedures (if activated, activities described in 2.4.3.5 would be performed in consultation and coordination with the CTU).

2.4.3.3.1 The **CTU will** conduct analysis focussed on the circumstances of the situation to determine the nature and scope of the incident.

2.4.3.3.2 The **CTU will** identify Primary and Supporting Departments and make a recommendation to the Management Team as to the key players for the response and recovery phases of the incident.

2.4.3.3.3 The **Royal Canadian Mounted Police will** proceed with a criminal investigation, concurrent with the GC response.

2.4.3.3.4 **National Defence will** proceed with a military options analysis and response, concurrent with the GC response, when there is a threat to its and the Canadian Forces systems or there is a cyber threat from any foreign military.

2.4.3.3.5 The **Canadian Security Intelligence Service will** proceed with an investigation, concurrent with the GC response, when there is a question of national security or a significant event.

2.4.3.3.6 **Communications Security Establishment Canada will**, concurrent with the GC response, monitor technological IT threats, provide technical threat and incident analysis and mitigation advice, and support investigations.

2.4.3.4 Engage Affected, Primary, and Supporting Departments to assist with the analysis.

2.4.3.5 Analyze the incident to identify the systems affected, the users affected, and the impact on business by:

2.4.3.5.1 Identifying the root cause of the incident (analysis may carry over into the recovery phase for complex incidents);

2.4.3.5.2 Analyzing the potential as well as the actual outcomes for the GC's critical services, assets, and infrastructures based on the Impact Severity Matrix (see Appendix C);

2.4.3.5.3 Assessing the likelihood of further spread or distributed impact of the incident based on available intelligence and threat assessments;

2.4.3.5.4 Prioritizing actions in the event that multiple incidents exist; and

2.4.3.5.5 Developing potential courses of action, each with its associated risks, anticipated level of effort, and timelines, to contain the incident and minimize the impact on other systems and services.

2.4.3.4 The **CCIRC will** work with a communications liaison (as needed).

2.4.3.5 The **CCIRC will** recommend the most appropriate courses of action and an associated response plan to the Management Team for review and approval.

2.4.4 Decision Points for the Response Course of Action

2.4.4.1 The **Management Team will** be the first level of executive management to direct the actions necessary to contain the incident quickly.

2.4.4.2 The **Management Team will** review the courses of action proposed by the CCIRC based on risk tolerance and the current GC environment and make its recommendation.

2.4.4.3 The **Management Team will** determine the communications plan. PS DG Communications will coordinate, direct, and lead the communications effort accordingly, potentially engaging the DG Comms WG.

2.4.4.4 Depending on the circumstances of the situation, the **Management Team may** decide to escalate the situation in the following manner:

2.4.4.4.1 Escalation to FERP response level 2 or 3, depending on the severity of the incident as defined in the Severity Impact Assessment Matrix in Appendix C;

2.4.4.4.2 Escalation to the executive committees, which include the following:

2.4.4.4.2.1 FCO,

2.4.4.4.2.2 ADM-EMC,

2.4.4.4.2.3 DMNS, and

2.4.4.4.2.4 Ops Committee.

2.4.4.5 The **Management Team will** approve decision briefs (where appropriate) and situation reports prepared by the GOC to advise the executive committees of the potential impact on service to Canadians, government operations, or confidence in government.

2.4.4.6 The **Management Team will** approve the response plan (see 2.4.3.7) in consultation with the executive committees.

2.4.4.7 The **Management Team will** direct the CCIRC, by way of the GOC, to coordinate the implementation of the GC-wide response plan. This may include, but is not limited to, notification of departments on specific response measures and the requirement to report back to the CCIRC, by way of the GOC, with a status report or situation report.

2.4.5 Implementation of the GC Response Plan

2.4.5.1 As directed by the Management Team, the **CCIRC will** coordinate, by way of the GOC, the implementation of the GC-wide response plan and work with departments to ensure the whole of the GC (where applicable) is aware of the situation at hand and prepared to deploy response measures as required.

2.4.5.2 Where applicable, the **CCIRC will** advise, by way of the GOC, departments of specific response measures and any requirements to report back to it, by way of the GOC, with a status report or situation report.

2.4.5.3 **Affected Departments** (and where applicable all departments) **will** work to implement any relevant GC response measures within their respective department.

2.4.5.4 **Departments will**, where applicable, report back to the CCIRC by way of the GOC (see 2.2.3.2.5).

2.4.5.5 The **CCIRC will** assess the residual risk utilizing the departmental situation reports and advise the Management Team of the risk, the situation, or changes in either based on this assessment.

2.4.5.6 The **CCIRC will** conduct ongoing situation and risk analysis to determine if the incident is contained within the identified Affected Departments and will report its findings to the Management Team.

2.4.5.6.1 In its risk assessment and situation report to the Management Team, the **CCIRC will** advise if the incident has been successfully contained. The CCIRC will also identify if any damage has been incurred or if normal operations have not resumed and, if so, the CCIRC will advise the Management Team to transition to the recovery phase (see 2.5.1) in parallel to the response phase.

2.4.6 Decision Points—Confirmation of Containment

2.4.6.1 The **Management Team will** review the risk assessment and situation report from the GOC against the analysis performed in coordination and consultation with the Affected Departments or other departments (where applicable).

2.4.6.2 The **Management Team will** brief the executive committees accordingly, depending on which, or if any, of the executive committees were engaged.

2.4.6.3 The engaged **executive committees** (as briefed by the Management Team) **will** decide if the incident has been contained based on the risk assessment and situation report.

2.4.6.4 The **Management Team will** decide whether or not to close the response stream or continue to monitor for specific or related threats or vulnerabilities.

2.5.6.4.1 If the decision is to continue the response stream and monitor specific or related incidents, any additional information will be validated and analyzed (see 2.4.3.2).

2.5.6.4.2 If the Management Team decides to close the stream, then post-incident analysis (see 2.6.1) will be conducted and there will be a return to the set of broad continuous processes of preparedness.

Inputs	Outputs
• Departmental incident and situation reports • Intelligence information (where applicable) • Criminal surveillance information (where applicable) • Significant event information (where applicable) • Publicly known vulnerabilities and threats • System logs (where applicable) • GC critical systems and services inventory • Technical resources • Political considerations • Legal considerations • Business objectives	• Detailed analysis of the incident • Situational awareness report (bidirectional from departments to the CCIRC and from the CCIRC to departments) • Response plan • Notification of executive management and engaged committees of the IMP • Establishment of the Augmented GOC through representatives from Primary and Supporting Departments • Containment of and response to the incident • Information products and RFIs • Where applicable, validated end to the threat, vulnerability, or incident

2.5 Recovery

Purpose

In recovery, the affected system, network, or service is restored to normal operations. In some instances, essential services may be temporarily restored to a degraded state as defined in BCPs. The recovery phase is concerned with issues that must be addressed and decisions that must be made after the immediate threat of the incident has subsided and the incident is contained.

Activities

2.5.1 Recovery Activation

2.5.1.1 The recovery phase is activated after the containment of an incident resulting in damage or disruption to normal operations.

2.5.1.2 If there was no resulting damage or disruption to normal operations, the **horizontal GC coordination (CCIRC) will** return to the set of broad continuous processes of preparedness.

2.5.2 Notification to the Management Team

2.5.2.1 The **CCIRC will** notify the Management Team of the information at hand regarding current damage or disruption to normal operations as well as the outcomes of the response measures, which were communicated in the departmental situation reports from the response phase (see 2.4.5.4).

2.5.2.1.1 The **head of the Management Team (PS's Director General, Operations Directorate) will** update the members of the Management Team (see 2.4.2.2).

2.5.3 Situational Awareness

2.5.3.1 **Affected Departments will** bring normal service levels back online and realign any interim service processes into normal operations.

2.5.3.2 The **CCIRC**, by way of the GOC, **is** the coordination point for the status of the GC recovery.

2.5.3.3 **Affected Departments will** provide situation report updates and verify to the GOC that normal operations have resumed.

2.5.3.4 Using these departmental situation report updates as input, the **CCIRC will**:

2.5.3.4.1 Develop recommendations and potential courses of action (where applicable) for the coordination of GC-wide recovery actions, in collaboration with Affected, Primary, and Supporting Departments still engaged from the response phase (see 2.4.3.4);

2.5.3.4.2 Work with the communications liaison (as needed); and

2.5.3.4.3 Recommend the most appropriate courses of action for recovery (the recovery plan) to the Management Team for review and approval.

2.5.4 Decision Points for the Recovery Course of Action

2.5.4.1 The **Management Team will** determine the communications plan. PS DG Communications will coordinate, direct, and lead the communications effort accordingly, potentially engaging the DG Comms WG.

2.5.4.2 Depending on the circumstances of the situation, the **Management Team may** decide to escalate the incident to the executive committees of the IMP.

2.5.4.3 The **Management Team will** approve decision briefs (where appropriate) and situation reports prepared by the GOC to advise the engaged executive committees of the impact on service to Canadians, government operations, or confidence in government and will propose recommendations for GC-wide recovery.

2.5.4.4 The **Management Team will** approve the recovery plan (see 2.5.3.4.3) in consultation with the engaged executive committees.

2.5.4.5 The **Management Team will** direct the CCIRC, by way of the GOC, to coordinate implementation of the GC-wide recovery plan.

2.5.5 Implementation of the GC Recovery Plan

2.5.5.1 As directed by the Management Team, the **CCIRC will** coordinate, by way of the GOC, the implementation of the GC-wide recovery plan and work with Affected Departments.

2.5.5.2 Where applicable, the **CCIRC will** advise, by way of the GOC, Affected Departments of specific GC recovery measures and any requirements to report back to the GOC with a status or situation report.

2.5.5.3 **Affected Departments** (and where applicable all departments) **will** work to implement any relevant GC recovery measures within their respective department.

2.5.5.4 **Departments will** report back to the CCIRC, by way of the GOC, on the status of their recovery efforts (where applicable).

2.5.5.5 The **CCIRC will** assess the GC recovery status based on the departmental situation reports and communicate its findings to the Management Team.

2.5.6 Decision Points—Confirmation of Recovery

2.5.6.1 The **Management Team will** review the GC recovery assessment and situation report provided by the CCIRC.

2.5.6.2 The **Management Team will** brief the engaged executive committees accordingly.

2.5.6.3 The engaged **executive committees will** decide if recovery throughout the GC has been achieved.

2.5.6.4 The **Management Team will** decide whether or not to close the recovery stream or continue to monitor the GC recovery efforts.

2.5.6.4.1 If the decision is to keep the stream open and continue to monitor recovery, additional departmental situation reports will be assessed and situational awareness will be updated accordingly (see 2.5.3.4).

2.5.6.4.2 If the Management Team decides to close the stream, then post-incident analysis (see 2.6) will be conducted and there will be a return to the set of broad continuous processes of preparedness.

Inputs	Outputs
• Updated situation reports from the Affected Department(s) • Draft information products	• GC-wide recovery plan • Information products (e.g. decision briefs, situational awareness reports) • GC service restoration

2.6 Post-Incident Analysis

Purpose

Post-incident analysis leverages knowledge gained from each incident to improve confidentiality, integrity, and availability of the GC IT infrastructure. By reviewing the results of mitigation, response, and recovery activities, the GC will identify areas for improvement with respect to its safeguards, processes, or policy instruments.

Activities

2.6.1 Observations and Recommended Actions

2.6.1.1 **Affected Departments will** contribute to the post-incident report prepared by the GOC (where applicable).

2.6.1.2 The **CCIRC will** assess the effectiveness of the processes and safeguards.

2.6.1.3 The **CCIRC will**, in consultation with the CTU and Affected and Supporting Departments, recommend areas for improvement and actions to mitigate future incidents.

2.6.2 Post-Incident Report

2.6.2.1 The **GOC will** produce a post-incident report.

2.6.2.2 **Affected Departments will** review the GOC post-incident report (where applicable).

2.6.2.3 **PS DG Communications will** coordinate, direct, and lead related communications activities.

2.6.2.4 The **Management Team** and its **executive committees** (as appropriate) will:

2.6.2.4.1 Ensure a post-incident report is produced; and

2.6.2.4.2 Approve the post-incident report.

2.6.3 GC Lessons Learned Action Plan

2.6.3.1 Based on the post-incident report, the **Secretariat CIOB**, in consultation with **PS, will** develop a comprehensive GC Lessons Learned Action Plan, including direction and recommendations to departments. The Action Plan may include the following:

2.6.3.1.1 Implementation of GC policy instruments and processes; or

2.6.3.1.2 Implementation of mitigating measures to improve GC IT security and safeguard IT availability.

2.6.3.2 The **Secretariat CIOB**, in collaboration with **PS, will** engage in follow-up to ensure the lessons learned are being applied.

2.6.3.3 The **Secretariat CIOB will** be the repository for post-incident reports.

2.6.3.4 The **Secretariat CIOB will** close the post-incident analysis phase of the GC IT IMP based on the implementation of mitigating measures and actions.

2.6.4 Implementation

2.6.4.1 **Affected Departments will** implement lessons learned (where applicable).

2.6.4.2 **Departments will** implement lessons learned (where applicable).

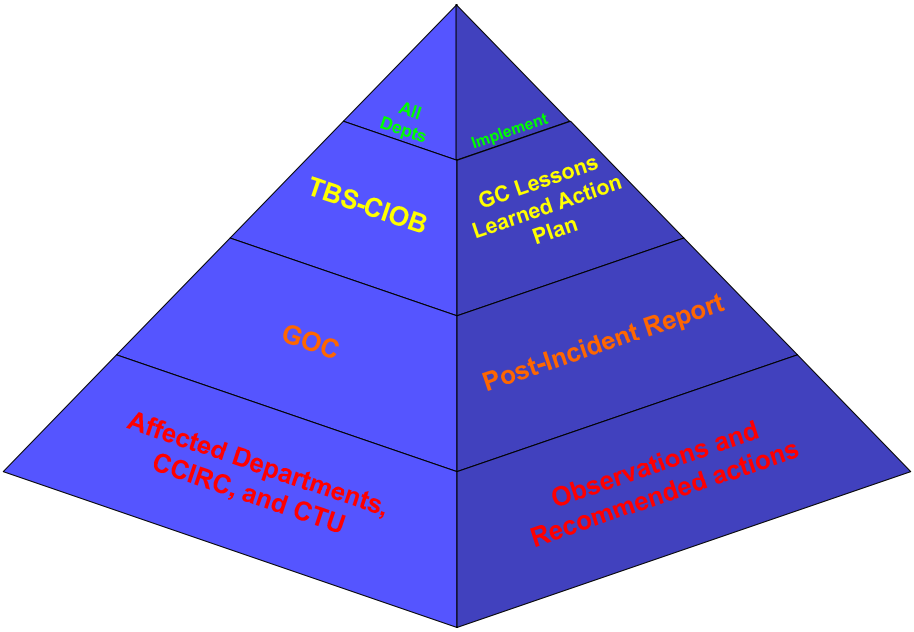

Figure 7: Post-Incident Analysis Activities

Inputs	Outputs
• Determining what went wrong and what worked according to plan • Reviewing the incident timeline • Reviewing the speed of notification and communication within the response phase and identifying areas of concern • Reviewing the root cause(s) of the problem • Determining the effectiveness of the incident's containment • Reviewing mitigating measures for security in order to prevent further incidents • Determining how the incident could have been prevented • Determining the complete impact (including costs, level of effort, and potential damage to reputation) of the incident on the GC and the Affected Department(s) • Identifying areas for improvement and for revision in GC policies, procedures, and processes	• Post-incident analysis • Post-incident report • GC Lessons Learned Action Plan

Appendix A: Acronyms

ADM	Assistant Deputy Minister
ADM-EMC	Assistant Deputy Minister Emergency Management Committee
ADM Security	Assistant Deputy Minister Security Committee
BCP	business continuity plan
CCIRC	Canadian Cyber Incident Response Centre
CIOB	Chief Information Officer Branch
CIOC	Chief Information Officer Council
CIO for the GC	Chief Information Officer for the Government of Canada
CTU	Cyber Triage Unit
DG Comms WG	Director General Communications Working Group
DMNS	Deputy Minister National Security Committee
EX	executive
FCO	Federal Coordinating Officer
FERMS	Federal Emergency Response Management System
FERP	Federal Emergency Response Plan
GC	Government of Canada
GC IT IMP	Government of Canada Information Technology Incident Management Plan
GOC	Government Operations Centre
IMP	Incident Management Plan
IT	information technology
ITS	information technology security

NATO	North Atlantic Treaty Organization
Ops Committee	Cabinet Operations Committee
PS	Public Safety
PS DG Communications	Public Safety Director General Communications
RFI	request for information
SA	situational awareness
Secretariat	Treasury Board of Canada Secretariat
Secretariat CIOB	Treasury Board of Canada Secretariat's Chief Information Officer Branch
SLA	service level agreement

Appendix B: Glossary

Advisories	Advisories are not as urgent as alerts but still describe security threats and issues (e.g. slowly spreading viruses or worms, major vulnerabilities in common software) that could affect the state of the GC's IT security and critical infrastructure. Advisories also contain mitigation advice.
Alerts	Alerts are extremely time sensitive and describe an immediate or active security issue. It is essential that they are sent out as quickly as possible. Examples of situations that would warrant an alert include public knowledge of an exploitable security vulnerability related to a previous PS advisory, rapidly spreading malicious code, an imminent threat against GC networks, or potential issues stemming from multiple denials of service.
Anomaly	An anomaly is anything that differs from expectation.[16] Anomaly is the neutral term used in place of other common descriptors such as bug, fault, failure, error, defect, problem, deviation, glitch, incident, or crash.
Canadian Cyber Incident Response Centre (CCIRC)	The CCIRC is responsible for monitoring threats and coordinating the national response to any cyber security incident. Its focus is the protection of national critical infrastructure against cyber incidents.
Cyber flashes	Cyber flashes are similar in urgency and content to advisories, yet they contain no official mitigation advice to address the vulnerability. Cyber flashes, unlike both alerts and advisories, are not publicly posted. They are therefore ideal for gathering information on new and emerging threats while avoiding unwanted publicity. Examples of cyber flashes include zero-day vulnerabilities or advance notification that a patch for a particular issue will soon be made available.
Decision briefs	Decision briefs are used to inform senior officials and ministers of the current issue, potential options for addressing that issue, and a recommended course of action for approval or review. Typically, a decision brief is complemented by a situation brief, which provides the context for the decision requested.

16 IEEE 1044-1993: Standard Classification for Software Anomalies, The Institute of Electrical and Electronics Engineers, Inc., N^{Y}, USA, 1994, page 1.

Event	An event is an observable change in the normal behaviour of a system, environment, process, workflow, or person (components).[17]
Government Operations Centre (GOC)	The GOC is Canada's strategic-level operations centre. It is the hub of a network of operations centres run by a variety of federal departments and deals with anything—real or perceived, imminent or actual, natural disaster or terrorist activity—that threatens the safety and security of Canadians or the integrity of Canada's critical infrastructure.
Incident handling	Incident handling includes the operational functions required to support a timely and orderly response to and recovery from an incident, such as communications, logistics, analysis, and coordination.
Incident management	The objective of incident management is to restore normal service operations as quickly as possible, minimize the adverse effect on business operations, and ensure the best possible levels of service, quality, and availability are maintained.[18] Incident management includes all aspects of incident handling as well as the strategic functions needed during an incident, such as leadership and decision making capabilities. Incident management ensures the ongoing provision of supporting services and activities required for timely and efficient incident handling.
Incident response	Incident response, which is typically technical in nature, includes those activities at the tactical level associated with the analysis, containment, and eradication of an incident. Incident response is situational in nature and depends on the characteristics of the incident.
IT incidents	An IT incident is understood to be: • Any event that disrupts the normal operations of an organization and causes or may cause a reduction in the quality of service or in productivity[19]; or • Any unauthorized attempt, whether successful or not, to gain access to, modify, destroy, delete, or render unavailable any computer network or system resource.

17 http://en.wikipedia.org/wiki/Computer_security_incident_management#Events

18 Details of the ITIL v2 framework, http://en.wikipedia.org/wiki/ITIL#Incident_Management

19 http://www.knowledgetransfer.net/dictionary/ITIL/en/Incident.htm

Notification	Notification provides initial information on an incident, risk assessment information, current information on response actions, and guidance on reporting requirements and public communications, which may include pre-scripted media lines. Depending on the nature of the incident, notification may be sent to members of the CIOC, IT security coordinators, and departmental security officers.
Shared services	Shared services refers to services that were previously spread across an organization or across sectors within that organization now being provided by one centralized group or sector within the organization—*sharing* within an organization or among sectors being the key concept.[20] Consequently, the funding and resourcing of the service is shared and the group, unit, or sector providing the service effectively becomes an internal service provider.
Situation report	A situation report provides current information pertaining to the incident and the immediate and future response actions. The report also includes an analysis of the impact and the identification of issues requiring attention.
Situational awareness	Situational awareness (SA) involves having insight into one's environment and circumstances to understand how events and actions will affect business objectives, both now and in the near future. Having complete, accurate, and current SA is essential in any domain where technological complexity, decision making, and the well-being of the public interact. Because incident management involves predictions and forecasts, SA in the area of IT requires an understanding of the interrelationships between critical services and information, safeguards supporting IT infrastructure and processes, and evolving threats.
Update	An update to any alert, advisory, or cyber flash can occur after it has been released. Updates are used to complement, correct, or update any of the electronic information products issued by the CCIRC to ensure that organizations involved in the management of vulnerabilities, threats, or incidents have all available information.
Common service organization	A common service organization is a department or organization, including a special operating agency, designated as a central supplier of particular services that support other departments.[21]

20 http://en.wikipedia.org/wiki/Shared_services

21 *Common Services Policy*, http://www.tbs-sct.gc.ca/pubs_pol/dcgpubs/TB_93/csp-psc01_e.asp#_Toc147652595

Appendix C: Impact Severity Assessment Matrix

The highest level achieved in all rows determines the level of impact on the GC.

Category	Impact Severity		
	Low Impact	**Medium Impact**	**High Impact**
Health and safety	No actual or potential impact on health and safety	Limited to moderate actual or potential impact on the health and safety of Canadians or employees	Life-threatening incidents or potentially life-threatening incidents
Scope of the incident	One or more departments	Limited number of departments	Numerous departments
Service delivery	Limited to no actual or potential impact on the GC's critical services or operations	Significant actual or potential impact on the GC's critical services or operations	Severe actual or potential impact on the GC's critical services or operations
Financial	Limited to moderate actual or potential financial impact (e.g. reduced productivity of public service employees)	Significant actual or potential financial impact (either to the GC or to its partners)	Severe actual or potential financial impact (either to the GC or to its partners)
Public confidence and GC reputation	Limited or no actual or potential impact on public confidence or GC reputation	Moderate actual or potential impact on public confidence or GC reputation	Significant actual or potential impact on public confidence or GC reputation

Appendix D: Incident Report Form

1.0 Reporting Entity

Name of organization:	

2.0 Contact Information

First name:		Initials:	
Last name:		Position:	
Phone:	( )	Cell:	( )
Pager:	( )	Fax:	( )
Email:			
Office address:			

3.0 Incident Description and Impact

Date and time of incident:	(date, time, and time zone)
Location of site affected by incident:	
(if more than one site is affected, please list)	
Estimated impact:	
Incident duration:	(if incident is over; otherwise, report 'ongoing')
Estimated number of systems affected:	
Percentage of departmental systems affected:	
Brief description of the incident:	

Actions taken:
(include date and time if possible)
Supporting documents attached:
(describe if any)

4.0 Status of Mitigation Actions

Mitigation details to date:	(list any actions that have been taken to mitigate incident and by whom)
Results of mitigation:	
Additional assistance required?	YES/NO

5.0 Incident Type

Malicious code	worm, virus, trojan, backdoor, rootkit
Known vulnerability exploit	*(list the CVE number for known vulnerability)*
System compromise	altering logs, altering DNS information
Data compromise	destroying data, altering data, Web defacement
Denial of service	DDoS, DoS
Access violation	unauthorized access attempt, successful unauthorized access, password cracking
Accident or error	equipment failure, operator error, user error, natural or accidental causes
Other or unknown	

6.0 Systems Affected

Network zone affected	Internet, DMZ, administration, internal, enclave
Type of system affected	file server, Web server, mail server, database, workstation, other (please specify)
Operating system (specify version)	Windows, Linux, Unix, MacOS, OS/390, other (please specify)
Protocols or services	(list all that apply)
Application	(include specific versions)

7.0 Apparent Origin of Incident or Attack

Source IP and port:		Protocol:	
URL:	(if any)	Malware:	(if any)

Note: Electronic data exchange details are available from the CCIRC.

Appendix E: Situation Report

SITUATION REPORT

Number: Event STXXX-08 (provided by the GOC)

Threat or event: Brief description of the threat or event

Date: Information valid as of XX:XX hours (EDT/EST)

Description of current threat or event:

- Summary of threat or event
- Background information on the event or incident
- Description of current conditions
- Current impacts on the population, government (facilities, services, assets), emergency response organizations, critical infrastructure (energy, utilities, IT, communications technology, finance, health care, food, water, transportation, safety, manufacturing), national security, law enforcement, the economy, and the environment

Report source(s): Original source of the report and any additional sources (media, regional offices, provincial emergency measures offices, other government organizations)

Current response actions: What is being done to respond to this event? (international, federal, provincial, territorial, or regional responses, responses of non-governmental organizations, conference calls, meetings, requests for provincial or federal assistance)

Future actions: What actions need to be taken or what issues require attention to respond to this event? What can be anticipated?

Assessment and analysis: The "so what" portion of the situation report. What do we know about the threat, existing vulnerabilities, and potential additional impacts? Any major issues should also be highlighted here.

Additional notifications:

Additional products:

Geomatics products:

Government Operations Centre (GOC)
Email: GOC-COG@ps-sp.gc.ca
Telephone: (613) 991-7000
Fax: (613) 996-0995
Secure Fax: (613) 991-7094

Appendix F: Decision Brief

Decision Brief

Delete this box—for instructional value only

The purpose of this report is to seek national policy direction from federal senior officials about an event or emergency.

This report will be printed and added to the Decision Brief Package under Tab 1.

Title

Title = name of the event taking place, i.e. ice storm, London bombing, Hurricane Katrina (delete—for instructional value only)

Threat or Event:

This should be a brief paragraph or a bulleted list describing the event or threat. The information in this section should be concise and specific to the event. Include all relevant geographic references and the date and time the event occurred. Ensure that standard or daylight savings time is correct. Format the time for the Eastern time zone, *not the time zone of the event's location*; indicate (EST) next to the time. Information in this section should be consistent with information in previously issued notifications and situation reports, if any have been issued for this event. (For this section, you may use the information found in the situation report's "Description of current threat or event" field.)

Background:

This section will provide explanatory information on the event taking place. This information (including illustrative information) is to be included under Tab 3 of the Decision Brief Package.

Current Status:

The status section will include a summary of situational awareness information (what is the situation *now*?), including known and potential impacts, relevant threat information, identification of vulnerabilities, extent of damage (impact on the public, geographical area affected), and aggravating factors (e.g. weather, critical infrastructure implications, availability of critical resources).

Current Actions:

Describe what actions are being executed at the present time by federal, provincial, territorial, and municipal governments and by the public sector:

- Notifications, warnings, or alerts issued
- Coordination efforts and key decision making
- Development of a strategic action plan
- Review of policy issues

Analysis and Assessment:

Provide a brief analysis and assessment of the event or threat, specific to the following areas:

- Financial costs
- Impact on federal-provincial and territorial relations
- Impact on international relations
- Potential deterioration of the incident
- Public confidence (media coverage)

Potential Course(s) of Action:

This section will include a description of each course of action that could be taken to respond to the situation at hand (as many options as are required).

- Option A: (description)
- Option B: (description)
- Option C: (descripton)

Prepared by:

Situational Awareness and Risk Assessment, Operations Directorate, Public Safety Canada

Appendix G: References and Further Reading

- Federal Emergency Response Plan
- *Government Security Policy*
- *Management of Information Technology Security Standard*
- www.publicsafety.gc.ca
- http://www.tbs-sct.gc.ca/pubs_pol/gospubs/tbm_12a/siglist_e.asp
- www.wikipedia.ca
- Article, Best-Practice Recommendations IT Incident Management, http://www.sun.com/emrkt/sunspectrum/Incd.Mgmt_Wht_ppr_5.22.pdf
- http://www.knowledgetransfer.net/dictionary/ITIL/en/Incident.htmpp