Treasury Board of Canada Secretariat Secrétariat du Conseil du Trésor du Canada

Canada

Government of Canada Cyber Security Event Management Plan (GC CSEMP) 2019

Published: 2020-05-11

Published by Treasury Board of Canada, Secretariat
90 Elgin, Ottawa, Ontario, K1A 0R5, Canada

Catalogue Number: BT22-182/2019E-PDF
ISBN or ISSN: 978-0-660-34801-8

This document is available on the Government of Canada website, Canada.ca

This document is available in alternative formats upon request.

Aussi offert en français sous le titre : Plan de gestion des événements de cybersécurité du gouvernement du Canada (PGEC GC) 2019

Government of Canada Gouvernement du Canada

Government of Canada Cyber Security Event Management Plan (GC CSEMP) 2019

From Treasury Board of Canada Secretariat

On this page

- 1.0 Preamble
- 2.0 Introduction
- 3.0 Government of Canada Cyber Security Event Management
- 4.0 Concept of Operations
- 5.0 Reporting and Communication
- Appendix A – Roles and Responsibilities
- Appendix B – Event Impact Assessment (Departmental)
- Appendix C – Response Level Calculation Matrix (GC (Government of Canada)-Wide)

1.0 Preamble

▼ In this section

- 1.1 About this document
- 1.2 Effective Date
- 1.3 Application
- 1.4 Definitions
- 1.5 Glossary of acronyms and abbreviations

1.1 About this document

This document describes the Government of Canada (GC) Cyber Security Event Management Plan (CSEMP). This plan outlines the stakeholders and actions required to ensure that cyber security events are addressed in a consistent, coordinated and timely fashion GC (Government of Canada)-wide. The plan will be tested and reviewed annually, and modified as required.

1.2 Effective Date

This plan takes effect on April 8, 2020. It replaces the version dated January 26, 2018.

1.3 Application

This plan is prepared in the exercise of the responsibilities conferred to the Treasury Board of Canada Secretariat (TBS) under the *Policy on Government Security* (PGS) and is intended for all departments and agencies subject to the PGS (Policy on Government Security).

1.4 Definitions

Note: These definitions are from the *Policy on Government Security*. Additional examples are provided for some terms to clarify their interpretation for the purposes of this plan.

Compromise:
A breach of government security. Includes but is not limited to:

- unauthorized access to, disclosure, modification, use, interruption, removal or destruction of sensitive information or assets, causing a loss of confidentiality, integrity, availability or value
- an event causing a loss of integrity or availability of government services or activities

Security event:
Any event, act, omission or situation that may be detrimental to government security, including threats, vulnerabilities and security incidents.

- Examples of cyber security events: Disclosure of a new vulnerability, intelligence that a threat actor may be planning an attack against a GC (Government of Canada) information system (for example, a distributed denial of service (DDoS) attack, attempts to breach the network perimeter)

Security incident:

Any event (or collection of events), act, omission or situation that has resulted in a compromise.

- Every cyber security incident is a cyber security event (or collection of cyber security events), but not every cyber security event is a cyber security incident (see Figure 1)
- Examples of cyber security incidents: Active exploitation of one or more identified vulnerabilities, exfiltration of data, failure of a security control, breach of a cloud-hosted or managed GC (Government of Canada) service

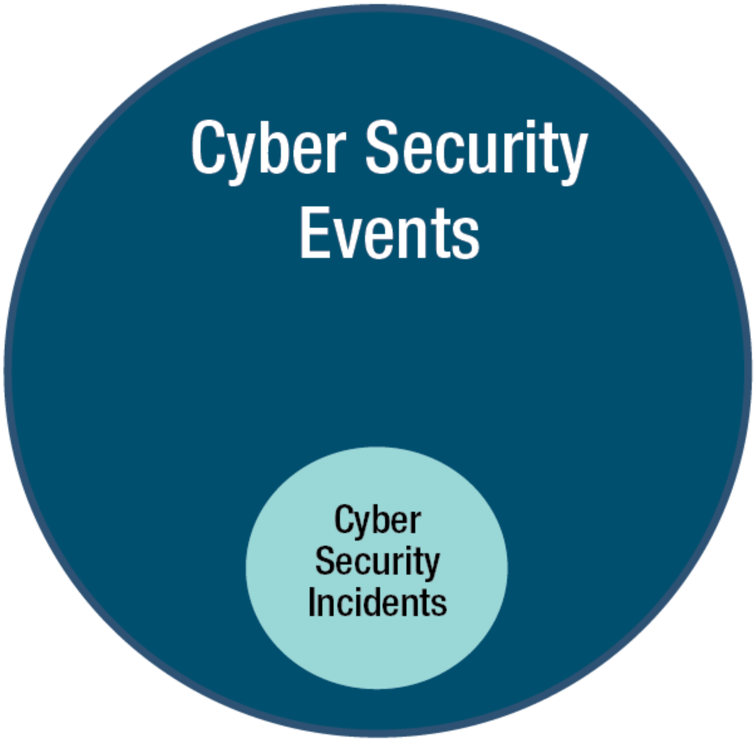
Threat:

Any potential event or act, deliberate or unintentional, or natural hazard that could result in a compromise.

Vulnerability:

A factor that could increase susceptibility to compromise.

Figure 1: Cyber security events versus incidents



▼ Figure 1 - Text version

Figure 1 identifies the difference between cyber security events and cyber security incidents as they are defined in the CSEMP through the use of two circles, one within the other. The first larger circle represents cyber security events, and the second much smaller circle within the first identifies cyber security incidents as being a subset of cyber security events.

1.5 Glossary of acronyms and abbreviations

ADM (Assistant Deputy Minister)	Assistant Deputy Minister
CCCS (Canadian Centre for Cyber Security)	Canadian Centre for Cyber Security, part of the Communications Security Establishment
CCNSS (Canadian Committee on National Security Systems)	Canadian Committee on National Security Systems
CIO (Chief Information Officer)	Chief Information Officer
Comms (Communications)	Communications
CSE (Communications Security Establishment)	Communications Security Establishment
CSEMP (Cyber Security Event Management Plan)	Cyber Security Event Management Plan
CSIS (Canadian Security Intelligence Service)	Canadian Security Intelligence Service
CSO (Chief Security Officer)	Chief Security Officer
DG (Director General)	Director General
DG ERC (Director General Event Response Committee)	Director General Event Response Committee
DND-CAF (National Defence/Canadian Armed Forces)	National Defence/Canadian Armed Forces
ECT (Event Coordination Team)	Event Coordination Team
EMT (Executive Management Team)	Executive Management Team

ERC (Event Response Committee)	Event Response Committee
FERP (Federal Emergency Response Plan)	Federal Emergency Response Plan
GC (Government of Canada)	Government of Canada
GOC (Government Operations Centre)	Government Operations Centre
IMOC (Incident Management and Operational Coordination)	Incident Management and Operational Coordination, part of the Canadian Centre for Cyber Security
IT (Information technology)	Information technology
ITSec (Information technology security)	Information technology security
LSA (Lead Security Agency)	Lead Security Agency
NSDS (Networks, Security and Digital Services)	Networks, Security and Digital Services, part of Shared Services Canada
NSS (National Security Systems)	National Security Systems
OCIO (Office of the Chief Information Officer)	Office of the Chief Information Officer, part of the Treasury Board of Canada Secretariat
PCO (Privy Council Office)	Privy Council Office
PS (Public Safety Canada)	Public Safety Canada
RCMP (Royal Canadian Mounted Police)	Royal Canadian Mounted Police
RFA (Request for Action)	Request for Action
S&I (Security and intelligence)	Security and intelligence
SC (Strategic communications)	Strategic communications
SCMA (Strategic Communications and Ministerial Affairs)	Strategic Communications and Ministerial Affairs, part of the Treasury Board of Canada Secretariat

SSC (Shared Services Canada)	Shared Services Canada
TBS (Treasury Board of Canada Secretariat)	Treasury Board of Canada Secretariat

2.0 Introduction

▼ **In this section**

- 2.1 Context
- 2.2 Purpose
- 2.3 Scope
- 2.4 Objectives
- 2.5 Assumptions

2.1 Context

Cyber security events related to Government of Canada (GC) information systems can have a significant impact on the delivery of government programs and services to Canadians and, consequently, confidence in government. The ability to respond to cyber security events in a consistent, coordinated and timely manner across the GC (Government of Canada) is essential to ensure the security and resilience of GC (Government of Canada) program and service delivery.

2.2 Purpose

The purpose of this document is to provide an operational framework for the management of cyber security events (including cyber threats, vulnerabilities or security incidents) that impact or threaten to impact the GC (Government of Canada)'s ability to deliver programs and services to Canadians. This document provides context for plans and procedures developed by departments and agencies to manage cyber security events related to the programs and services for which they are responsible.

This document also complements the all-hazards arrangements and response mechanism of the Federal Emergency Response Plan (FERP) to provide a coherent framework for managing the consequences of cyber events affecting multiple government institutions, confidence in government, or both.

2.3 Scope

The scope of this plan is limited to cyber security events (including threats, vulnerabilities or security incidents) on GC (Government of Canada) information systems classified as Secret and below that either:

- affect or may affect delivery of government programs and services to Canadians, government operations, security or privacy of information or confidence in government
- require an integrated GC (Government of Canada)-wide response to minimize impacts and enable prompt mitigation and restoration of government programs and services

This plan does not address:

- cyber security events impacting Top Secret information systems
- the coordination of cross-jurisdictional cyber security events (for example, with provinces, territories, municipalities, other countries or non-governmental organizations)

2.4 Objectives

The objectives of this cyber security event management plan are to:

- enhance situational awareness of likely cyber threats and vulnerabilities, as well as confirmed cyber security incidents, across the GC (Government of Canada)
- improve cyber event coordination and management within the GC (Government of Canada)
- mitigate threats and vulnerabilities before a compromise can occur
- support GC (Government of Canada)-wide cyber risk assessment practices and remediation prioritization efforts

- minimize the impacts of cyber events to the confidentiality, availability or integrity of government programs and services, information and operations
- inform decision-making at all necessary levels
- improve sharing and exchange of GC (Government of Canada) knowledge and expertise
- enhance public confidence in the GC (Government of Canada)’s ability to manage cyber security events

2.5 Assumptions

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

- all departments and agencies have event management processes and business continuity plans in place as established under the Policy on Government Security
- responsibilities of GC (Government of Canada) cyber security stakeholders are established in accordance with current departmental mandates
- cyber security events related to the disclosure of personal information or private communications will also follow established privacy protocols
- federal cyber security events impacting multiple jurisdictions (national or international) are coordinated in accordance with national plans issued by Public Safety Canada

3.0 Government of Canada Cyber Security Event Management

▼ **In this section**

- 3.1 Process overview
- 3.2 Stakeholders
- 3.3 GC (Government of Canada) response levels
  - 3.3.1 Determination of GC (Government of Canada) response levels
- 3.4 Governance
  - 3.4.1 Event Coordination Team
  - 3.4.2 Executive Management Team

- 3.4.3 ADM (Assistant Deputy Minister) IT (Information Technology) Security Tripartite Committee
- 3.4.4 Escalation model
- 3.4.5 Escalation and response levels
- 3.4.6 De-escalation

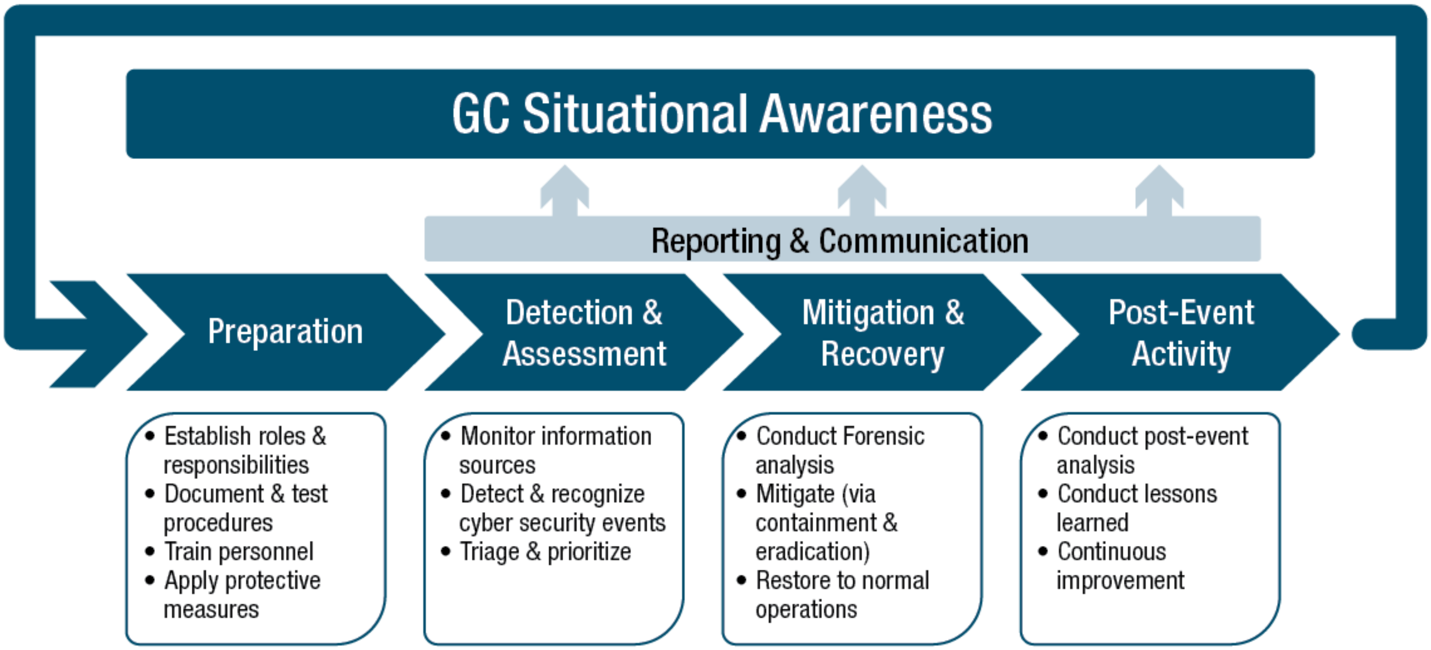
Government security and the continuity of GC (Government of Canada) programs and services rely upon the ability of departments and agencies, as well as government as a whole, to manage cyber security events. All government departments experience events that either impact or threaten to impact the delivery of government programs and services. As the GC (Government of Canada) is increasingly dependent upon IT (Information technology) to deliver services to Canadians and maintain operations, it needs to be prepared to react quickly and effectively to any event that may adversely affect services to Canadians, government operations or confidence in government.

The GC (Government of Canada) Cyber Security Event Management Plan (GC CSEMP) outlines the stakeholders and actions required to ensure that cyber security events are addressed in a consistent, coordinated and timely fashion GC (Government of Canada)-wide. This section of the plan outlines the cyber security event management process, identifies implicated stakeholders, defines cyber security event response levels and describes escalation triggers.

3.1 Process overview

The overall cyber security event management process defined in this document has several phases, as outlined in Figure 2.

Figure 2: Cyber Security Event Management Process


GC Situational Awareness
Reporting & Communication
Preparation
Detection & Assessment
Mitigation & Recovery
Post-Event Activity
• Establish roles & responsibilities
• Document & test procedures
• Train personnel
• Apply protective measures
• Monitor information sources
• Detect & recognize cyber security events
• Triage & prioritize
• Conduct Forensic analysis
• Mitigate (via containment & eradication)
• Restore to normal operations
• Conduct post-event analysis
• Conduct lessons learned
• Continuous improvement

▼ Figure 2 - Text version

Figure 2 represents the overall cyber security event management process and its multiple phases, as defined in this document. The four phases (preparation, detection and assessment, mitigation and recovery, and post-event activity) are depicted in the middle, with an arrow pointing from the final phase (post-event activity) back to the first (preparation) to indicate a continuous feedback loop. Under each key phase is a short description. The descriptions read as follows:

1. Preparation
   a. Establish roles and responsibilities
   b. Document and test procedures
   c. Train personnel
   d. Apply protective measures
2. Detection and assessment
   a. Monitor information sources
   b. Detect and recognize cyber security events
   c. Triage and prioritize
3. Mitigation and recovery
   a. Conduct forensic analysis
   b. Mitigate (via containment and eradication)
   c. Restore to normal operations
4. Post-event activity

a. Conduct post-event analysis
b. Conduct lessons learned
c. Continuous improvement

Above phases 2 to 4 is a box that contains the words reporting and communication. This indicates that reporting is an ongoing activity throughout these phases. This box has arrows pointing up to a box that contains the words GC situational awareness to represent the central concept of ongoing situational awareness across the GC at every point in the event management lifecycle.

The initial phase, preparation, involves general readiness activities to ensure that the GC (Government of Canada) is ready to respond to the broad range of cyber security events. In this phase, event-related roles and responsibilities are established, plans and procedures are documented (or updated with lessons learned) and exercised, and personnel are trained. A key component of this phase also includes the application of protective and preventive measures at the host, application and network levels. Protective measures also include the implementation of vulnerability management, patch management and other related processes.

The second phase, detection and assessment, involves the discovery of potential cyber security events, including confirmed cyber security incidents, through the monitoring of various information sources (including departmental and GC (Government of Canada)-wide hardware and software solutions) and submission of reports by affected departments and agencies. This phase also includes an initial assessment of event impact levels that feed into the determination of an appropriate GC (Government of Canada) response.

The third phase, mitigation and recovery, consists of all response actions required to minimize impacts to confidentiality, availability and integrity, and lead to restoration of normal operations. Containment and eradication are key components of this phase, which includes, but is not limited to, actions such as shutting down systems, disconnecting from networks, disabling functionality, and mitigating exploited vulnerabilities via patch installation. Recovery actions in this phase include invocation of business continuity or disaster recovery plans, or any other measure that will reduce impact to affected information systems and allow for a return to normal operations. This phase also includes root cause analysis and investigation, which consist of activities such as evidence gathering, forensic analysis, research and other related processes that could influence recovery actions.

The final phase, post-event activity, is vital for continuous improvement of the overall cyber security event management process and, as such, feeds back into the preparation phase to complete the event management life cycle. This phase consists of post-event analysis, preparing and reviewing event lessons learned, and recommending changes to processes or procedures in order to continually mature the GC (Government of Canada)’s cyber security event management capability.

From the time that an event is detected to the conclusion of post-event activities, reporting and communication between stakeholders occurs throughout, enabling whole-of-government situational awareness. Entrenching these ongoing activities into the life cycle of cyber security event management is imperative to ensure that mitigation advice and status updates are shared with both affected and non-affected parties in a timely fashion, enabling situational awareness and supporting informed decision-making.

3.2 Stakeholders

In addition to individual departments and agencies, which play a key role in informing and taking action on GC (Government of Canada) cyber security event management activities, a number of other stakeholders are also involved in the GC (Government of Canada) CSEMP (Cyber Security Event Management Plan). Below is a summary of stakeholders, organized into three major categories. Detailed roles and responsibilities of each stakeholder can be found in Appendix A.

GC (Government of Canada) CSEMP (Cyber Security Event Management Plan) stakeholders

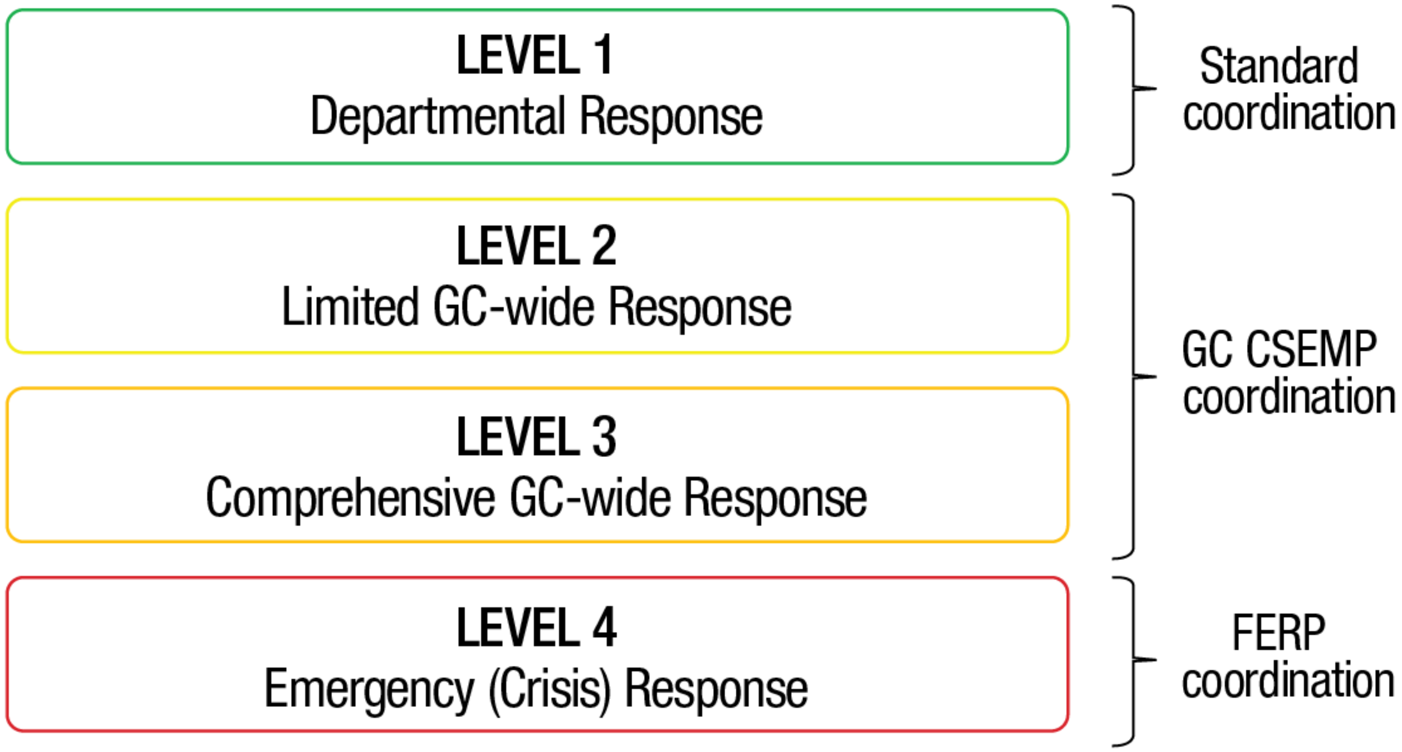
1. **Primary stakeholders**
    - Treasury Board of Canada Secretariat (TBS)
        - Office of the Chief Information Officer (OCIO)
        - Strategic Communications and Ministerial Affairs (SCMA)

   - Canadian Centre for Cyber Security (CCCS), part of the Communications Security Establishment (CSE)
      - Incident Management and Operational Coordination (IMOC)
      - Communications (Comms)
2. **Specialized stakeholders**
   - Royal Canadian Mounted Police (RCMP)
   - Canadian Security Intelligence Service (CSIS)
   - National Defence/Canadian Armed Forces (DND-CAF)
   - Shared Services Canada (SSC)
      - Networks, Security and Digital Services (NSDS)
      - Service Delivery Management
      - Public Safety Canada, National Cyber Security Directorate (NCSD)
3. **Other stakeholders**
   - GC (Government of Canada) Chief Information Officer (GC CIO)
   - Government Operations Centre (GOC)
   - Privy Council Office (PCO)
      - Security and Intelligence (S&I)
      - Strategic Communications (SC)
   - Canadian Committee on National Security Systems (CCNSS)
   - DG (Director General) Event Response Committee (DG ERC)
   - External Partners

3.3 GC (Government of Canada) response levels

There are four response levels that govern GC (Government of Canada) cyber security event management activities, as indicated in Figure 3. These response levels will dictate the level of coordination required in response to any given cyber security event, including level of escalation, stakeholder participation and reporting required.

Figure 3: GC (Government of Canada) response levels



▼ Figure 3 - Text version

Figure 3 represents the four GC response levels that govern GC cyber security event management activities and dictate the necessity and degree of enterprise response required. The figure uses four stacked boxes with the level of required coordination identified to the right of the boxes.

1. Level 1 – Departmental response
    a. Requires standard coordination
2. Level 2 – Limited GC-wide response
    a. Requires GC CSEMP coordination
3. Level 3 – Comprehensive GC-wide response
    a. Requires GC CSEMP coordination
4. Level 4 – Emergency (crisis) response
    a. Requires FERP coordination

Level 1 essentially represents day-to-day operations in the GC (Government of Canada). The dynamic nature of the cyber threat environment and the constant disclosure of new cyber security vulnerabilities indicate that, on average, the GC (Government of Canada) will typically operate in a Level 1 state. In this state, departments and agencies are to coordinate response in accordance with their standard departmental procedures, continue the application of regular preventive measures and maintain communication with the Canadian Centre for Cyber Security (CCCS)'s Incident Management and Operational Coordination (IMOC) Group for advice and guidance. At a GC (Government of Canada)-wide level, no further coordination among primary or specialized stakeholders is required, aside from regular information-sharing between stakeholders for situational awareness.

Level 2 indicates that heightened attention is required at the GC (Government of Canada) level. This level will trigger invocation of the lower tier of GC (Government of Canada) CSEMP (Cyber Security Event Management Plan) governance (as outlined in section 3.4.4) and implies that some limited GC (Government of Canada)-wide coordination may be required. At this level, all primary GC (Government of Canada) CSEMP (Cyber Security Event Management Plan) stakeholders (and specialized stakeholders, when required) will be on heightened alert for cyber activity, monitoring GC (Government of Canada)-wide risk levels and ensuring that any impact or potential impact is contained and mitigated. Additional targeted advice to departments and agencies on how to proceed with an event response, which could include invocation of emergency patch management processes.

Level 3 indicates that immediate focus and action is required at the GC (Government of Canada) level. This level will trigger invocation of the upper tier of GC (Government of Canada) CSEMP (Cyber Security Event Management Plan) governance (as outlined in subsection 3.4.4) and implies that centralized, GC (Government of Canada)-wide coordination will be required. At this level, event response will be fully coordinated via the GC (Government of Canada) CSEMP (Cyber Security Event Management Plan) governance structure, with departments and agencies given ongoing direction and guidance on how to proceed with event response. Response may range from invocation of emergency patch management processes to the disconnection of systems from GC (Government of Canada) networks. Events at this level will also trigger invocation of TBS (Treasury Board of Canada Secretariat)'s Cyber Security Communications Framework [1].

Level 4 is reserved for severe or catastrophic events that affect multiple government institutions, confidence in government or other aspects of the national interest. Events that reach this level will immediately shift to the FERP (Federal Emergency

Response Plan) governance structure, coordinated by the GOC (Government Operations Centre) in accordance with the FERP (Federal Emergency Response Plan), in order to ensure the harmonization of federal response efforts.

3.3.1 Determination of GC (Government of Canada) response levels

GC (Government of Canada) response levels are determined based on the analysis of two factors: Departmental impact assessment and scope of the cyber security event in question.

Departmental impact assessments are conducted using the process outlined in Appendix B of this document. This process, applicable to all cyber security events in scope of this plan, is based on a standardized injury test designed to measure the degree of injury that has occurred or could reasonably be expected to occur due to a compromise. This injury assessment considers both the severity and scope of the event. Once the degree of injury is assessed, a modifier is applied to account for the probability of injury realization in cases where an incident has not yet occurred (for example, unrealized cyber threats and vulnerabilities).

Departmental impact assessment results from affected departments are then rolled up at the GC (Government of Canada)-wide level and Appendix C of this document is then used by the CCCS (Canadian Centre for Cyber Security)-IMOC (Incident Management and Operational Coordination) (in collaboration with TBS (Treasury Board of Canada Secretariat)'s Office of the Chief Information Officer (TBS (Treasury Board of Canada Secretariat)-OCIO (Office of the Chief Information Officer)) and other applicable partners) to assess the GC (Government of Canada)-wide urgency and establish an appropriate GC (Government of Canada) response level.

Note: In some cases (such as the disclosure of a new security vulnerability for which injury is difficult to discern), more detailed departmental impact assessments may be required in order to establish a GC (Government of Canada) response level. In these cases, departments will be instructed to perform a detailed assessment via a CCCS (Canadian Centre for Cyber Security)-IMOC (Incident Management and Operational Coordination) Request for Action (RFA) and submit results back to the

CCCS (Canadian Centre for Cyber Security)-IMOC (Incident Management and Operational Coordination) to feed GC (Government of Canada) response level determination.

3.4 Governance

During a cyber security event, the timely engagement of the appropriate level of governance bodies will focus both management and operations to prevent, detect, respond to and recover from cyber security events in a prioritized manner.

The GC (Government of Canada) CSEMP (Cyber Security Event Management Plan) governance structure introduces three key governance bodies that will manage escalation of a cyber security event: the Event Coordination Team (ECT), the Executive Management Team (EMT) and the ADM (Assistant Deputy Minister) IT (Information technology) Security Tripartite (ADM ITST). When a cyber event occurs, the lead minister for the response will be determined on a case-by-case basis, according to the unique context of the event.

3.4.1 Event Coordination Team

The Event Coordination Team (ECT) is a group of key working-level stakeholders that is activated when triggered by the GC (Government of Canada) CSEMP (Cyber Security Event Management Plan) (Level 2 events) or when invoked by the Executive Management Team (EMT) (Level 3 events) or DG (Director General) Event Response Committee (DG ERC) (Level 4 events). The purpose of the ECT (Event Coordination Team) is to collaborate with key stakeholders and jointly propose recommendations for appropriate courses of action for the GC (Government of Canada) at large. The ECT (Event Coordination Team) is also responsible for ensuring that situational awareness is maintained at the DG (Director General) level by actively updating EMT (Executive Management Team) members of ongoing cyber security event management progress.

The ECT (Event Coordination Team) is co-chaired by TBS (Treasury Board of Canada Secretariat)-OCIO (Office of the Chief Information Officer) and CCCS (Canadian Centre for Cyber Security)-IMOC (Incident Management and Operational Coordination), with stakeholder representation varying depending on the nature of the event. As a primary stakeholder, TBS (Treasury Board of Canada Secretariat)-SCMA (Strategic Communications and Ministerial Affairs) will participate, along with the co-chairs, in responding to all types of cyber security events (cyber threats, vulnerabilities and security incidents).

When a cyber security incident is confirmed, or when a cyber threat event falls within the scope of other mandates, the team will expand to include the following specialized stakeholders, as required:

- SSC (Shared Services Canada) (Networks, Security and Digital Services)
- Public Safety (National Cyber Security Directorate)
- RCMP (Royal Canadian Mounted Police) (Technical Investigation Services and Federal Policing)
- CSIS (Canadian Security Intelligence Service) (Cyber)
- DND-CAF (National Defence/Canadian Armed Forces) (Information Management Operations)

Departments directly affected by specific threats or incidents will also be invited to participate on the ECT (Event Coordination Team). Departmental invitations will be determined by the co-chairs, who may limit invitations to ensure optimal operation of the ECT (Event Coordination Team).

During Level 4 events, the ECT (Event Coordination Team) co-chairs will ensure that a subject matter expert is co-located in the GOC (Government Operations Centre) to provide advice and guidance and ensure that situational awareness is maintained.

3.4.2 Executive Management Team

The Executive Management Team (EMT) is a DG (Director General)-level committee that is activated when triggered by the GC (Government of Canada) CSEMP (Cyber Security Event Management Plan) (Level 3 events). The EMT (Executive Management Team) provides strategic direction and guidance to the ECT (Event Coordination Team) and presents products to senior GC (Government of Canada) officials (such as decision briefs or proposed GC (Government of Canada)-wide mitigation plans that require approval at the ADM (Assistant Deputy Minister) level). The EMT (Executive Management Team) is also responsible for ensuring that situational awareness is maintained at higher levels by actively updating appropriate ADM (Assistant Deputy Minister) committees. During Level 4 events, the EMT (Executive Management Team) is integrated within the FERP (Federal Emergency Response Plan)'s DG (Director General) ERC (Event Response Committee).

The EMT (Executive Management Team) is co-chaired by TBS (Treasury Board of Canada Secretariat)-OCIO (Office of the Chief Information Officer) and CCCS (Canadian Centre for Cyber Security)-IMOC (Incident Management and Operational Coordination), with stakeholder representation varying depending on the nature of the event. As a primary stakeholder, TBS (Treasury Board of Canada Secretariat)-SCMA (Strategic Communications and Ministerial Affairs) will participate, along with the co-chairs, in responding to all types of cyber security events (cyber threats, vulnerabilities and security incidents). When a cyber security incident is confirmed, or when a cyber threat event falls within the scope of other mandates, the team will expand to include the following specialized stakeholders, as required:

- Government Operations Centre (GOC)
- Public Safety (NCSD (National Cyber Security Directorate))
- RCMP (Royal Canadian Mounted Police) (Technical Investigation Services and Federal Policing)
- CSIS (Canadian Security Intelligence Service) (Cyber)
- SSC (Shared Services Canada) (NSDS (Networks, Security and Digital Services))
- DND-CAF (National Defence/Canadian Armed Forces) (Information Management Operations)

Departments directly affected by specific threats or incidents will also be invited to participate on the EMT (Executive Management Team). Departmental invitations will be determined by the co-chairs, who may limit invitations to ensure optimal operation of the EMT (Executive Management Team).

3.4.3 ADM (Assistant Deputy Minister) IT (Information technology) Security Tripartite Committee

The ADM (Assistant Deputy Minister) IT (Information technology) Security Tripartite Committee (ADM ITST) is an ADM (Assistant Deputy Minister)-level committee that serves as a decision-making body supporting the effective design, delivery and management of priority IT (Information technology) security initiatives affecting internal GC (Government of Canada) systems and GC (Government of Canada)-wide operations. In the context of cyber security event management, its activation may be triggered by the GC (Government of Canada) CSEMP (Cyber Security Event Management Plan) (Level 3 events). The ADM (Assistant Deputy Minister) ITST provides mitigation direction and guidance to the EMT (Executive Management Team) when responding to a cyber security event. The ADM (Assistant Deputy Minister) ITST is also responsible for ensuring that situational awareness is maintained at higher levels by actively updating appropriate DMs. During Level 4 events, the ADM (Assistant Deputy Minister) ITST will support the FERP (Federal Emergency Response Plan)'s Committee of Assistant Deputy Ministers as appropriate.

The ADM (Assistant Deputy Minister) ITST is chaired by the Chief Technology Officer (CTO) at TBS (Treasury Board of Canada Secretariat)-OCIO (Office of the Chief Information Officer), and its primary members are CSE (Communications Security Establishment)'s Deputy Chief at CCCS (Canadian Centre for Cyber Security) and the ADM (Assistant Deputy Minister) at SSC (Shared Services Canada)-NSDS (Networks, Security and Digital Services). Other stakeholder representation at ADM (Assistant Deputy Minister) ITST will vary depending on the nature of the event. As a primary stakeholder, TBS (Treasury Board of Canada Secretariat)-SCMA (Strategic Communications and Ministerial Affairs) will participate, along with the co-chairs, in responding to all cyber security types of events (cyber threats, vulnerabilities and security incidents).

When a cyber security incident is confirmed, or when a cyber threat event falls within the scope of other mandates, the team will expand to include the following specialized stakeholders, as required:

- Government Operations Centre (GOC)
- Public Safety (National and Cyber Security Branch)
- SSC (Shared Services Canada) (Service Delivery Management)
- RCMP (Royal Canadian Mounted Police) (Technical Investigation Services and Federal Policing)

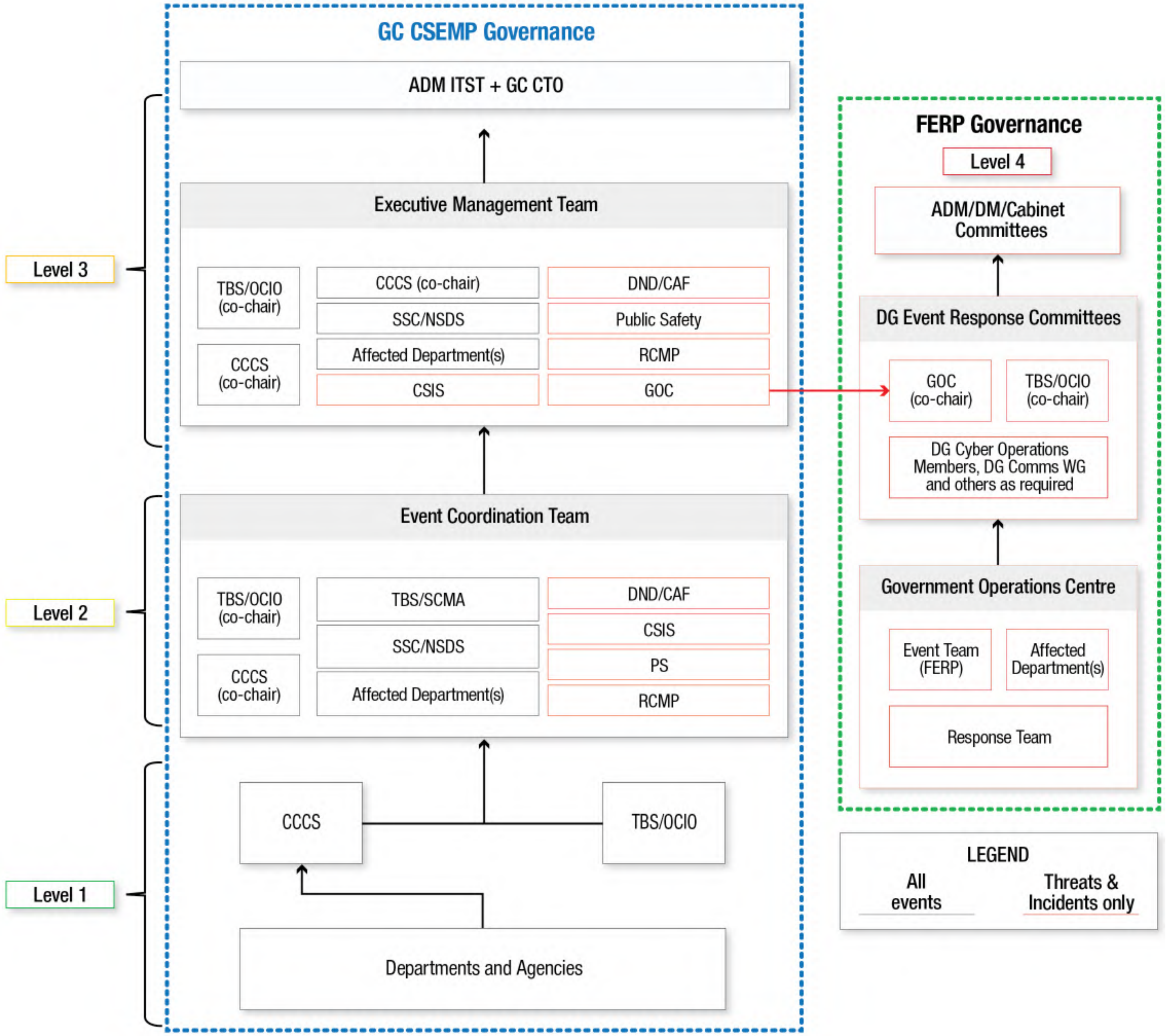
- DND-CAF (National Defence/Canadian Armed Forces) (Chief of Staff Information Management Group)
- CSIS (Canadian Security Intelligence Service)
- Affected departments and agencies

3.4.4 Escalation model

The escalation model of the GC (Government of Canada) CSEMP (Cyber Security Event Management Plan), outlined in Figure 4, identifies both the working-level and senior management stakeholders required, differentiating between primary and specialized members that vary based on event type (reflected by the black and red outlines). Appropriate governance bodies (either the ECT (Event Coordination Team), the EMT (Executive Management Team) or both) will be invoked, as required, by any stakeholder following analysis of data received from affected organizations. It should be noted that this model identifies the minimum subset of stakeholders that must be involved in escalation; co-chairs of each governance body can invite other GC (Government of Canada) organizations as appropriate (for example, a specialized stakeholder from whom information originated).

Given the short time frames in which cyber security events can cause significant damage, rapid invocation of the appropriate governance body is essential. As such, the initial invocation of each respective governance body is dependent on the GC (Government of Canada) response level established for that particular event. For example, should an event be assessed at a Level 3 from the outset, governance will immediately begin at the EMT (Executive Management Team) level.

Figure 4: GC (Government of Canada) CSEMP (Cyber Security Event Management Plan) escalation model



▼ Figure 4 - Text version

Figure 4 represents the CSEMP escalation model. This figure identifies the required governance based on the response level identified in figure three. Figure four identifies the working level and senior management stakeholders required, differentiating between primary and specialized members who vary based on event type. They are as follows:

1. Level 1 – Departmental response
   a. This level falls under GC CSEMP governance
   b. Departments and agencies provide information to CCCS for all events
   c. CCCS will then relay this information to TBS-OCIO

2. Level 2 – Limited GC-wide response
    a. This level falls under GC CSEMP governance
    b. An event at this level invokes the Event Coordination team (invoked by CCCS and/or TBS-OCIO). This team is made up of the following working-level members:
        i. TBS-OCIO (co-chair)
        ii. CCCS (co-chair)
        iii. Public Safety (National Cyber Security Directorate)
        iv. TBS-SCMA (TBS communications)
    c. In scenarios where a threat or incident has been identified, the following members will join the Cyber Security Event Management team:
        i. RCMP
        ii. DND-CAF
        iii. CSIS
        iv. the affected department(s)
3. Level 3 – Comprehensive GC-wide response
    a. This level falls under GC CSEMP governance
    b. An event at this level invokes the Executive Management team, which is made up of the following DG-level members:
        i. TBS-OCIO (co-chair)
        ii. CCCS (co-chair)
        iii. Public Safety
        iv. TBS-SCMA (TBS communications)
    c. In scenarios where a threat or incident has been identified, the following members will join the Executive Event Management team:
        i. RCMP
        ii. DND-CAF
        iii. GOC (who acts as the Executive Event Management team liaison to the FERP governance structure if the incident required further escalation)
        iv. CSIS
        v. the affected department(s)

    d. In level three, the GC-CIO and other ADM-level committees (which are intentionally flexible because engagement will vary based on the type of event) are identified as stakeholders and will be provided information by the Executive Event Management team

4. Level 4 – Emergency (crisis) response
    a. This level falls under FERP governance
    b. This level is active in the case of threats and incidents only
    c. There are three identified governance bodies in this level, which inform from the bottom up in the following order:
        i. Government Operations Centre (working-level)
            1. Cyber Security Event Management team
            2. Event team (FERP)
            3. affected departments
        ii. DG Event Response Committee (DG-level)
            1. GOC (co-chair)
            2. TBS-OCIO (co-chair)
            3. DG Cyber Operations Members, DG Communications working group, and others as required
        iii. ADM, DM, Cabinet Committees

Following are other notes about the escalation model:

- For **all** events:
    - stakeholders in the lower levels of the escalation model are engaged (or remain active, if already engaged) when higher levels are engaged during an event
    - stakeholders in higher levels of the escalation model, even if not formally engaged, are provided with appropriate situational awareness updates throughout the life cycle of an event
- For **Level 2** events:
    - ECT (Event Coordination Team) invocation implies that implicated stakeholders are simply in communication with one another and does not necessarily require that members formally convene in person

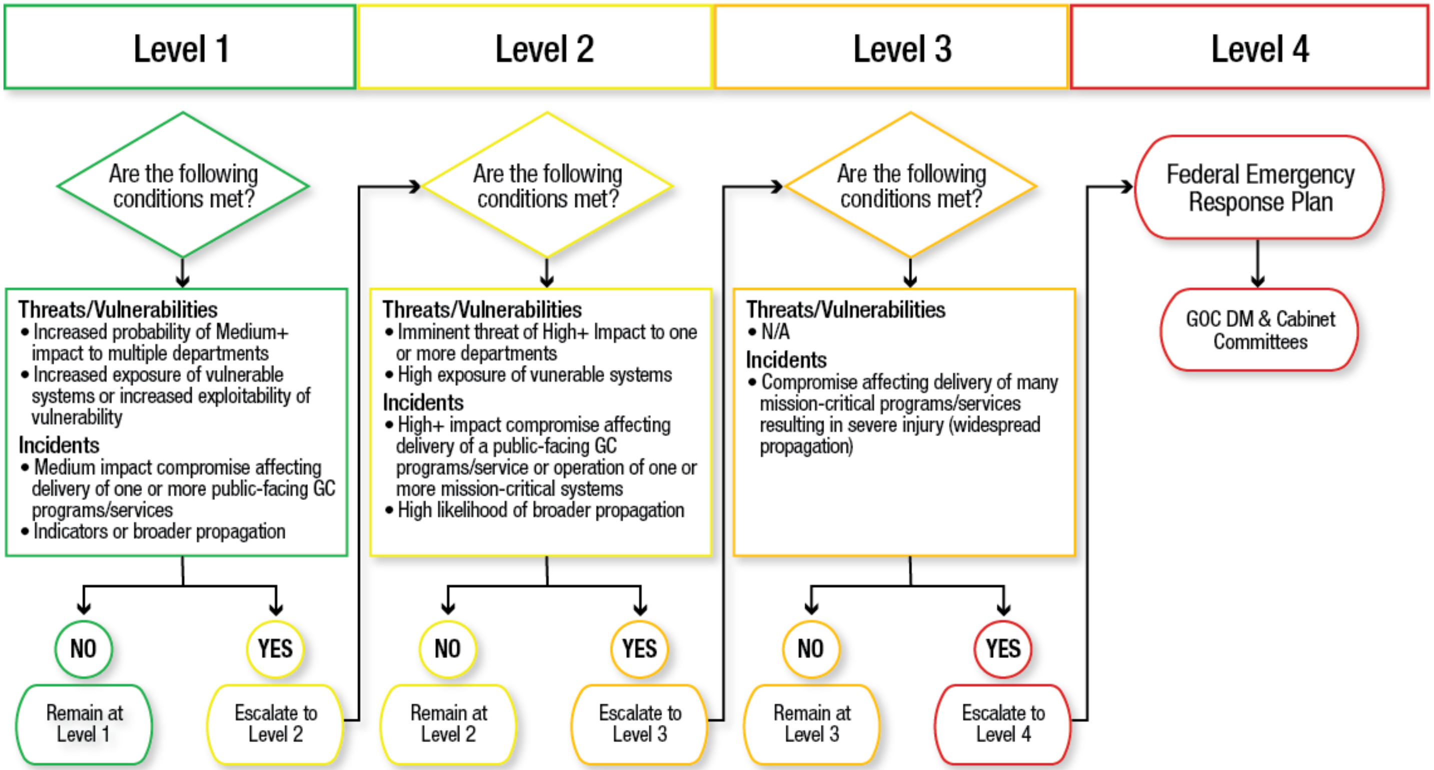
    - the ECT (Event Coordination Team) will escalate if mitigation efforts need to be augmented, if greater event impact is realized or if event context dictates heightened GC (Government of Canada) response
- For **Level 3** events:
    - EMT (Executive Management Team) invocation implies that implicated stakeholders convene formally in person
    - the decision to escalate and move to FERP (Federal Emergency Response Plan) response coordination will be made by DG (Director General) GOC (Government Operations Centre), in consultation with the EMT (Executive Management Team)
- For **Level 4** events:
    - GC (Government of Canada) CSEMP (Cyber Security Event Management Plan) stakeholders will remain engaged with the FERP (Federal Emergency Response Plan) event teams and will continue to fulfill their respective mandates within the GC (Government of Canada), aligned with direction provided via FERP (Federal Emergency Response Plan) governance
    - existing information-sharing mechanisms will be used as much as possible to maintain efficiency

3.4.5 Escalation and response levels

Stakeholders also need to be aware that GC (Government of Canada) response levels can change as an event unfolds depending on whether certain criteria are met. Figure 5 illustrates triggers for escalation that can be used during an event in order to invoke the appropriate stakeholders at the appropriate times. Escalation from one level to the next is determined jointly by the stakeholders involved, using injury (or potential injury) to the GC (Government of Canada) as a trigger (based on the results from the injury test outlined in Appendix B). Other escalating factors may also need to be considered, based on the context of the event in question.

Depending on the nature of the event, injury tests may need to be re-evaluated in order to accurately assess the level of escalation required. For cyber threat and vulnerability events, escalation would be triggered based on an increase in exposure to injury (for example, increased likelihood of occurrence, increased exploitability or exposure of vulnerable systems, decreased effectiveness of security controls). For confirmed cyber security incidents, escalation would be triggered based on an increase in severity or scope of the injury.

Figure 5: Escalation and response levels


Level 1
Level 2
Level 3
Level 4
Are the following conditions met?
Threats/Vulnerabilities
• Increased probability of Medium+ impact to multiple departments
• Increased exposure of vulnerable systems or increased exploitability of vulnerability
Incidents
• Medium impact compromise affecting delivery of one or more public-facing GC programs/services
• Indicators or broader propagation
NO
YES
Remain at Level 1
Escalate to Level 2
Are the following conditions met?
Threats/Vulnerabilities
• Imminent threat of High+ Impact to one or more departments
• High exposure of vunerable systems
Incidents
• High+ impact compromise affecting delivery of a public-facing GC programs/service or operation of one or more mission-critical systems
• High likelihood of broader propagation
NO
YES
Remain at Level 2
Escalate to Level 3
Are the following conditions met?
Threats/Vulnerabilities
• N/A
Incidents
• Compromise affecting delivery of many mission-critical programs/services resulting in severe injury (widespread propagation)
NO
YES
Remain at Level 3
Escalate to Level 4
Federal Emergency Response Plan
GOC DM & Cabinet Committees

▼ Figure 5 - Text version

Figure 5 identifies relevant stakeholders and the associated triggers for escalation for the various government response levels identified in figure two through the use of concentric circles and an attached table. The triggers for escalation are as follows:

1. Level 1 – Departmental response
   a. Stakeholders
      i. Day-to-day operations of:
         1. Departments and agencies
         2. CCCS
   b. Triggers for escalation
      i. Threats and vulnerabilities
         1. Increased probability of medium or higher impact to multiple departments

2. Increased exposure of vulnerable systems or increased exploitability of vulnerability

ii. Incidents

1. Medium-impact compromise affecting delivery of one or more public facing GC programs and services
2. Indicators of broader propagation

2. Level 2 – Limited GC-wide response
   a. Stakeholders
      i. Event Coordination team
   b. Triggers for escalation
      i. Threats and vulnerabilities
         1. Imminent threat of high or higher impact to one or more departments
         2. High exposure of vulnerable systems
      ii. Incidents
         1. High or higher impact of compromise affecting delivery of a public-facing GC programs and services or operation of one or more mission-critical systems
         2. High likelihood of broader propagation
3. Level 3 – Comprehensive GC-wide response
   a. Stakeholders
      i. Executive Management team
      ii. ADM committees (as required)
      iii. GC CIO
   b. Triggers for escalation
      i. Threats and vulnerabilities
         1. N/A
      ii. Incidents
         1. Compromise affecting delivery of many mission-critical programs and services resulting in severe injury (widespread propagation)
4. Level 4 – Emergency (crisis) response
   a. Stakeholders

        i. Federal Emergency Response Plan
            1. GOC
            2. DM and Cabinet committees
    b. Triggers for escalation
        i. N/A

3.4.6 De-escalation

GC (Government of Canada) response levels can be reduced as an event unfolds depending on whether mitigation measures are effective, if an incident is determined to be less severe than originally believed, if the threat is reduced or if the vulnerability of government systems is determined to be lessened. The decision to de-escalate from one level to the next is made by the committee co-chairs, in consultation with stakeholders involved, using injury (or potential injury) to the GC (Government of Canada) as a trigger (based on the results from the injury test outlined in Appendix B). Other de-escalating factors may also need to be considered, depending on the context of the event in question.

Depending on the nature of the event, injury tests may need to be re-evaluated in order to accurately assess the level of response required. For cyber threat and vulnerability events, de-escalation will be triggered based on a decrease in exposure to injury (for example, less likelihood of occurrence, decreased exploitability or exposure of vulnerable systems, increased effectiveness of security controls). For confirmed cyber security incidents, de-escalation will be triggered based on a decrease in severity or scope of the injury.

4.0 Concept of Operations

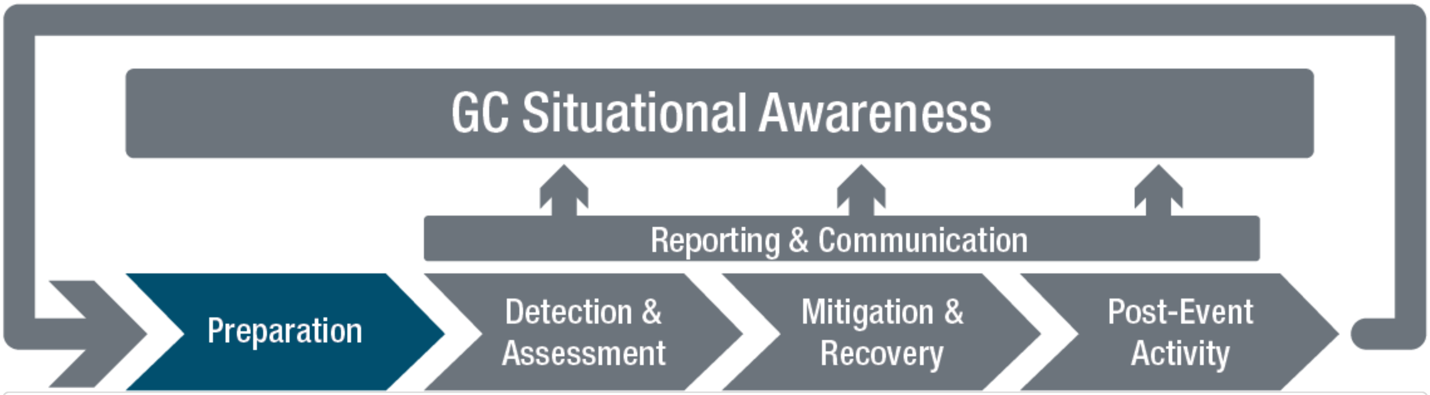
▼ **In this section**

- 4.1 Preparation
- 4.2 Detection and assessment
- 4.3 Mitigation and recovery
- 4.4 Post-event activity

The following subsections provide an overview of stakeholder expectations for each phase of the GC (Government of Canada) cyber security event management life cycle. These subsections will demonstrate how the GC (Government of Canada) CSEMP (Cyber Security Event Management Plan) is operationalized, and describe the key inputs and outputs from each phase.

All stakeholders are responsible for developing their own standard operating procedures or internal processes to deliver the expected outputs.

4.1 Preparation



▼ Figure Preparation - Text version

This is a repeat of figure 2, with all but the preparation arrow in the colour grey. The preparation arrow is highlighted in the colour blue and this image is a visual representation of the phase being described for the reader in this section.

The preparation phase is an ongoing phase in which the GC (Government of Canada) executes a set of continuous processes in order to ensure proactive readiness for specific or unpredictable events. This phase includes the maintenance and improvement of existing capabilities and the development of new mechanisms for setting priorities, integrating multiple organizations and functions, and ensuring that the appropriate means are available to support the full spectrum of cyber security event management requirements. This phase also includes the application of protective and preventive measures in advance of a cyber event.

In this phase:

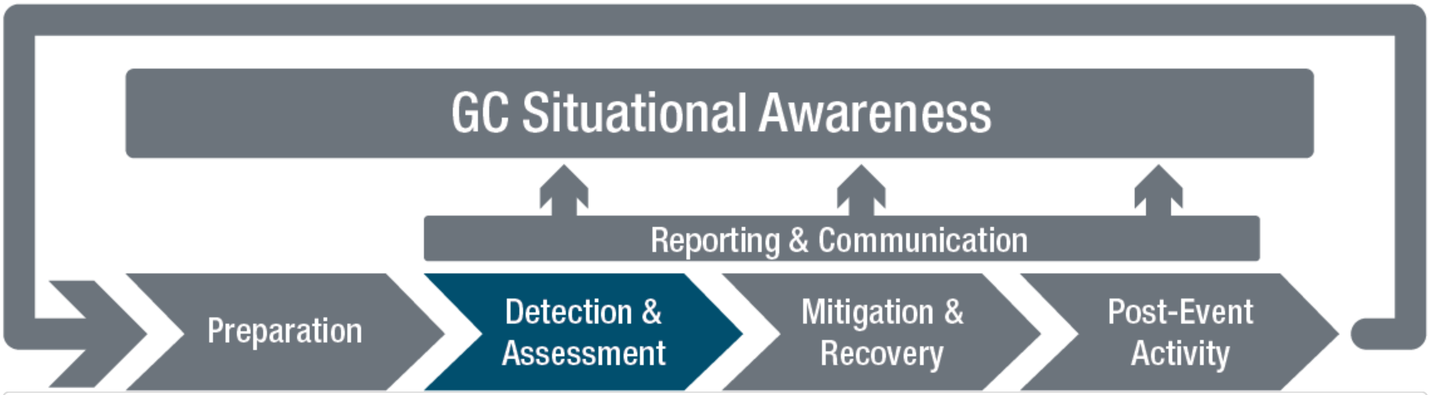
- **all GC (Government of Canada) CSEMP (Cyber Security Event Management Plan) stakeholders (including all departments and agencies)** will implement applicable protective and preventive measures within their respective areas of responsibility, in accordance with advice and guidance issued by lead security agencies (LSAs)
- **TBS (Treasury Board of Canada Secretariat)** will develop and maintain the GC (Government of Canada) CSEMP (Cyber Security Event Management Plan), coordinate regular exercises with all implicated stakeholders and ensure that lessons learned are implemented
- **TBS (Treasury Board of Canada Secretariat)** will review post-mortem and lessons-learned reports from past events and drive changes to security policy or enterprise security reference architectures, as required
- **CCCS (Canadian Centre for Cyber Security)-IMOC (Incident Management and Operational Coordination)** will maintain GC (Government of Canada)-wide operational distribution lists and ensure that departments and agencies are continually provided with advice and guidance required to mitigate cyber threats and vulnerabilities in order to prevent the occurrence of cyber security incidents
- **Departments and agencies, including service providers such as SSC (Shared Services Canada)**, will align departmental plans, processes and procedures with the GC (Government of Canada) CSEMP (Cyber Security Event Management Plan), participate in exercises when required and ensure that applicable government-wide lessons learned are implemented at the departmental level
- **Departments and agencies, including service providers such as SSC (Shared Services Canada)**, will continually maintain a list of their mission-critical information systems

Inputs and outputs for this phase are as follows:

- **Inputs**
  - Lessons learned from previous events, mitigation strategies, exercises and test scenarios
  - Ongoing recommendations from LSA (Lead Security Agency)s
  - Industry best practices

- **Outputs**
    - Implemented lessons learned
    - Updated GC (Government of Canada)-wide cyber security event management plans, processes, guidelines and tools
    - Exercises, scenarios and tests to validate the effectiveness of the GC (Government of Canada) CSEMP (Cyber Security Event Management Plan)
    - Updated departmental plans, processes and procedures that align with the GC (Government of Canada) CSEMP (Cyber Security Event Management Plan)
    - Understanding of critical systems across the GC (Government of Canada)

4.2 Detection and assessment



▼ Figure Detection and assessment - Text version

This is a repeat of figure 2, with all but the detection and assessment arrow in the colour grey. The Detection and Assessment arrow is highlighted in the colour blue and this image is a visual representation of the phase being described for the reader in this section.

The detection and assessment phase involves the continuous monitoring of information sources for early indications of emerging cyber security events and the assessment of their impact (potential or actual) on the delivery of services to Canadians, government operations or confidence in government.

The detection portion of this phase is constant for any type of cyber event (threat, vulnerability or security incident) and also covers the initial notification of appropriate stakeholders. Detection occurs as a direct result of monitoring; if the monitoring component is inadequate or incomplete, then the detection process may miss anomalies or events that could impact the GC (Government of Canada).

In the detection portion of this phase:

- **Primary and specialized GC (Government of Canada) CSEMP (Cyber Security Event Management Plan) stakeholders** will monitor their respective information sources for precursors of emerging cyber threat or vulnerability events, or indicators of potential or confirmed cyber security incidents, and **immediately notify the CCCS (Canadian Centre for Cyber Security)-IMOC (Incident Management and Operational Coordination)** of any malicious cyber activity that may affect GC (Government of Canada) information systems. Specifically:
  - CCCS (Canadian Centre for Cyber Security)-IMOC (Incident Management and Operational Coordination) will monitor:
    - technical sources and information reported by other stakeholders
    - the GC (Government of Canada) perimeter and all endpoints for which they have visibility
    - department-operated cloud-based environments, including endpoints or services within their purview
    - government networks and intelligence sources
    - information from domestic and international sources
  - **RCMP (Royal Canadian Mounted Police)** will monitor information from criminal surveillance sources
  - **CSIS (Canadian Security Intelligence Service)** will monitor information from intelligence sources
  - **DND-CAF (National Defence/Canadian Armed Forces)** will monitor all DND-owned and -operated networks, as well as networks from allied sources (such as NATO), and when deployed on operation
- **Primary and specialized GC (Government of Canada) CSEMP (Cyber Security Event Management Plan) stakeholders** will, upon detection of a cyber event, report cyber security events to applicable organizations, as per subsection 5.1 of this plan

- **Departments and agencies, including service providers such as SSC (Shared Services Canada),** will implement the general security controls established under the *Policy on Government Security* on IT (Information technology) infrastructure for which they are responsible and notify the CCCS (Canadian Centre for Cyber Security)-IMOC (Incident Management and Operational Coordination) upon detection of a cyber security event, as per the reporting requirements outlined in subsection 5.2 of this plan
- **Departments and agencies, including service providers such as SSC (Shared Services Canada)**, will notify appropriate law enforcement or national security authorities when information is received indicating that an event would fall under these particular domains, as per subsection 5.2.3 of this plan

The assessment portion of this phase begins once information has been received that a potential or actual cyber security event may exist. The purpose of the assessment phase is to establish a GC (Government of Canada) response level and determine whether invocation of GC (Government of Canada) CSEMP (Cyber Security Event Management Plan) or FERP (Federal Emergency Response Plan) governance is required.

In the assessment portion of this phase:

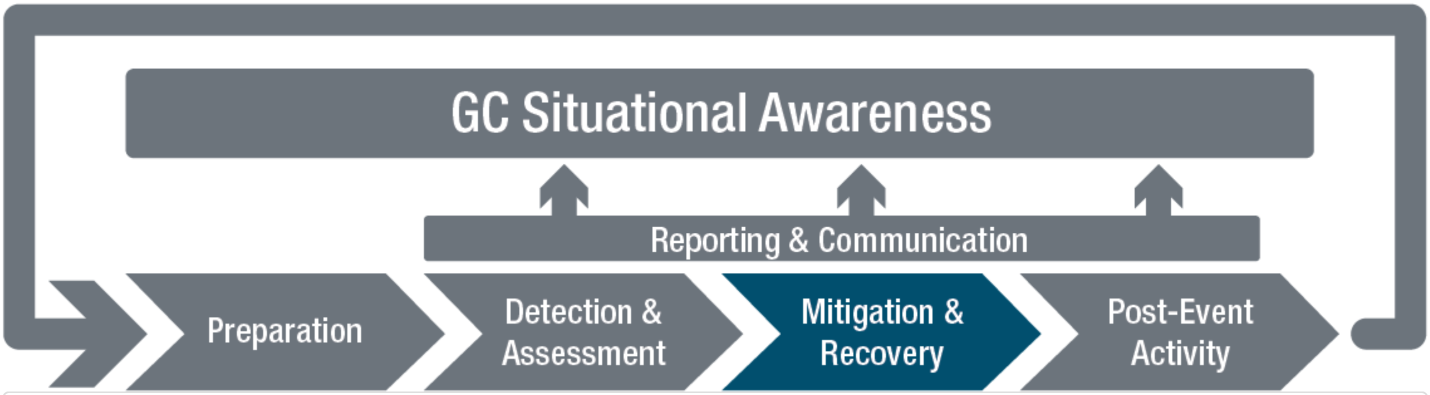
- **CCCS (Canadian Centre for Cyber Security)-IMOC (Incident Management and Operational Coordination)** will establish the initial GC (Government of Canada) response level, in consultation with TBS (Treasury Board of Canada Secretariat)-OCIO (Office of the Chief Information Officer) and other applicable partners, based on a roll-up of departmental information, and invoke the appropriate GC (Government of Canada) CSEMP (Cyber Security Event Management Plan) governance bodies in accordance with the assessed response level
    - **When further information is required to assess GC (Government of Canada)-wide risk:**
        - **CCCS (Canadian Centre for Cyber Security)-IMOC (Incident Management and Operational Coordination)** will leverage, where possible, automated tools to gather information required to support an impact assessment

- **CCCS (Canadian Centre for Cyber Security)-IMOC (Incident Management and Operational Coordination)** will issue a Request for Action (RFA) to departments and agencies, in consultation and concurrence with TBS (Treasury Board of Canada Secretariat)-OCIO (Office of the Chief Information Officer), to perform a departmental impact assessment
- **Departments and agencies** will perform a departmental impact assessment and submit results back to the CCCS (Canadian Centre for Cyber Security)-IMOC (Incident Management and Operational Coordination) within the defined time frame

Inputs and outputs for this phase are as follows:

- **Inputs**
  - Threat and intelligence reports from GC (Government of Canada) event management stakeholders or external sources (vendors, open source, etc.)
  - Incident reports from GC (Government of Canada) event management stakeholders, departmental incident reports or external sources
- **Outputs**
  - Departmental and government-wide impact assessment reports
  - Establishment of a GC (Government of Canada) response level
  - Identification of events that require a coordinated GC (Government of Canada)-wide response
  - Invocation of GC (Government of Canada) CSEMP (Cyber Security Event Management Plan) or FERP (Federal Emergency Response Plan) governance, if required

4.3 Mitigation and recovery



▼ Figure Mitigation and recovery - Text version

This is a repeat of figure 2, with all but the mitigation and recovery arrow in the colour grey. The mitigation and recovery arrow is highlighted in the colour blue and this image is a visual representation of the phase being described for the reader in this section.

The purpose of the mitigation and recovery phase is to mitigate threat and vulnerability events before they become incidents, or to contain and mitigate the effects of incidents when they occur. Activities in this phase will vary depending on the nature of the event, but could include actions such as the installation of patches, implementation of preventive measures, containment and eradication of a confirmed incident (which may involve investigative analysis), the invocation of business continuity and disaster recovery plans or the temporary shutdown of vulnerable services. Regardless of the type of event, the end goal of the phase is to minimize impacts and ensure the timely restoration of normal operations.

In this phase, for all applicable events (note that the degree of involvement will vary based on the established GC (Government of Canada) response level):

- **TBS (Treasury Board of Canada Secretariat)-OCIO (Office of the Chief Information Officer)** will perform strategic coordination, which may include the issuance of strategic direction to departments and agencies on measures to minimize the GC (Government of Canada)-wide impact of cyber security events (for example, shutting down vulnerable public-facing information systems, invoking disaster recovery plans) (Level 3 events or when warranted by Level 2 events).

- **GOC (Government Operations Centre)** will perform strategic coordination, which may include the issuance (via TBS (Treasury Board of Canada Secretariat)-OCIO (Office of the Chief Information Officer)) of strategic direction to departments and agencies on measures to minimize the GC (Government of Canada)-wide impact of cyber security events (Level 4 events only).
- **CCCS (Canadian Centre for Cyber Security)-IMOC (Incident Management and Operational Coordination)**, as a defensive service provider, will perform operational coordination, which includes issuing technical direction and advice to departments and agencies on measures to mitigate or contain impact to departmental systems (for example, patch installation, blocking of IP addresses), and tracking and reporting these measures (all events).
- **All primary and specialized GC (Government of Canada) CSEMP (Cyber Security Event Management Plan) stakeholders** will contribute advice and guidance based on information received from their respective sources.
- **Departments and agencies, including service providers such as SSC (Shared Services Canada)**, will implement the direction provided by CCCS (Canadian Centre for Cyber Security)-IMOC (Incident Management and Operational Coordination) and TBS (Treasury Board of Canada Secretariat)-OCIO (Office of the Chief Information Officer) within established timelines (on devices and infrastructure for which they are responsible). Service providers, such as SSC (Shared Services Canada), will liaise with their client departments to coordinate infrastructure patching (all events).

In addition, for confirmed incidents (all Level 3+ and applicable Level 2):

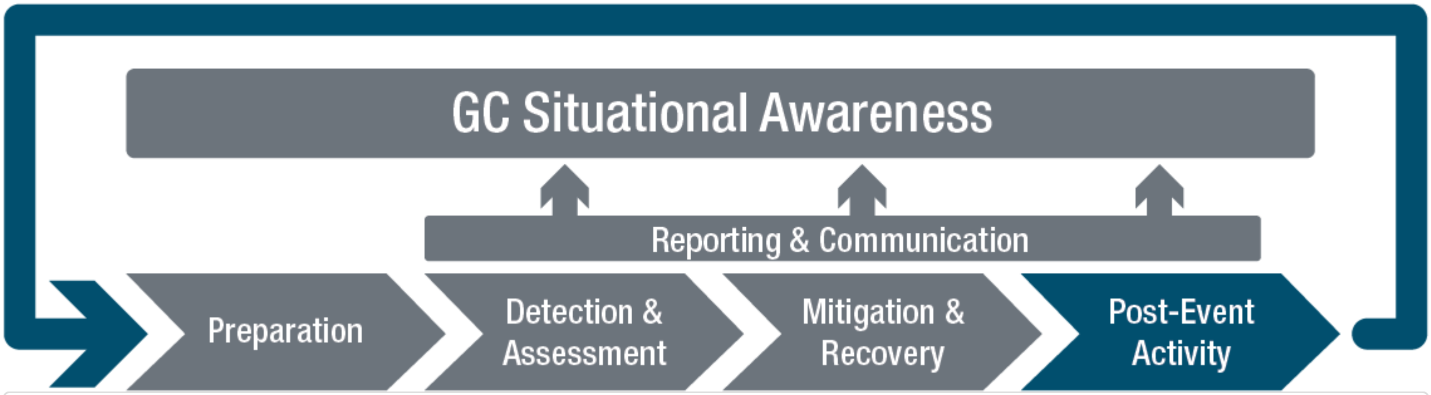
- CCCS (Canadian Centre for Cyber Security)-IMOC (Incident Management and Operational Coordination) will:
  - lead the development of a GC (Government of Canada)-wide containment plan, in collaboration with GC (Government of Canada) CSEMP (Cyber Security Event Management Plan) stakeholders
  - leverage their collection capabilities to facilitate a targeted response
  - help implement the prevention or containment plan in their respective areas of responsibility

    - lead forensic examination and analysis (including evidence collection) on IT (Information technology) systems that it supports, in collaboration with affected departments, agencies and applicable LSAs
- **Applicable service providers and affected departments and agencies** will help implement the prevention or containment plan in their respective areas of responsibility
- **SSC (Shared Services Canada)-NSDS (Networks, Security and Digital Services)** will help identify and report on affected or vulnerable systems to facilitate a targeted approach to mitigation activities, in collaboration with departments and agencies

Inputs and outputs for this phase are as follows:

- **Inputs**
    - Incident and situation reports
    - Intelligence information
    - Forensic findings
    - Other considerations (political, legal, and so on)
    - Impact assessment reports
    - Business continuity plans/disaster recovery plans
- **Outputs**
    - Response plan
    - Mitigation of threat or vulnerability (when applicable)
    - Containment and eradication of incident (when applicable)
    - Restoration to normal operations
    - Validated end to threat, vulnerability or incident

4.4 Post-event activity



▼ Figure Post-event activity - Text version

This is a repeat of figure 2, with all but the post-event activity and feedback arrows in the colour grey. The post-event activity and feedback arrows are highlighted in the colour blue and this image is a visual representation of the phase being described for the reader in this section.

The post-event activity phase leverages knowledge gained from each cyber security event to ensure the continual improvement of the cyber security event management process and, by extension, the security posture of the GC (Government of Canada) infrastructure as a whole. The purpose of this phase is to formally close out the cyber security event by conducting a post-event analysis, identifying lessons learned (when applicable) and driving changes to security policy or enterprise security architecture improvements, as required.

The degree of effort and resources allocated to this phase will vary from event to event. Serious events (including confirmed incidents) will require deeper post-event analysis than those that are less serious in nature. Repetitive events may require post-event analysis in aggregate.

In this phase, for applicable events (or upon request):

- **affected departments and agencies** will produce their own departmental lessons-learned report and action plan, and contribute to GC (Government of Canada)-wide post-event activities, as required
- **CCCS (Canadian Centre for Cyber Security)-IMOC (Incident Management and Operational Coordination)** will collate all departmental findings and

produce a post-event report, including a timeline of events and root cause analysis
- **TBS (Treasury Board of Canada Secretariat)-OCIO (Office of the Chief Information Officer)** will produce a lessons-learned report and action plan on behalf of the GC (Government of Canada) and monitor implementation of the recommendations (Level 3 events or when warranted by Level 2 events)
- **GOC (Government Operations Centre)** will produce a lessons-learned report and provide coordination for the production of departmental action plans and monitor the implementation of the recommendation (Level 4 events only)
- **all other GC (Government of Canada) CSEMP (Cyber Security Event Management Plan) stakeholders** will provide information required to support the development of GC (Government of Canada)-wide lessons-learned reports and assist with implementation of related action items under their particular areas of responsibility

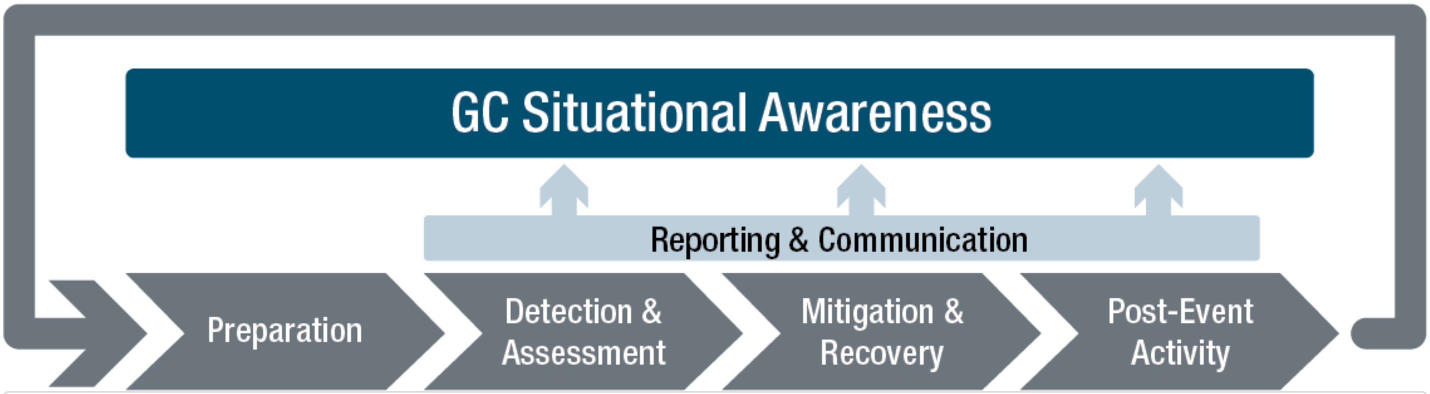
Inputs and outputs for this phase are as follows:

- **Inputs**
  - Review of event timeline
  - Review of reporting and communication procedures and timeliness of products
  - Root cause analysis
  - Other relevant input from implicated CSEMP (Cyber Security Event Management Plan) stakeholders
- **Outputs**
  - Departmental lessons-learned report
  - GC (Government of Canada)-level post-event reports
  - GC (Government of Canada)-wide lessons learned and action plan (if applicable)
  - Recommendations to improve policy instruments or enterprise security architecture

5.0 Reporting and Communication

▼ In this section

- 5.1 Government-wide reporting and communication
  - 5.1.1 Reporting and communication summary
- 5.2 Departmental reporting requirements
  - 5.2.1 Threat or vulnerability events
  - 5.2.2 Incidents
  - 5.2.3 Reporting examples
  - 5.2.4 Other
- 5.3 Secure communications



▼ Figure Reporting and Communication - Text version

This is a repeat of figure 2, with all but the GC situational awareness and reporting and communication boxes in the colour grey. The GC situational awareness and reporting and communication boxes are highlighted in the colour blue and this image is a visual representation of the phase being described for the reader in this section.

As cyber security events are detected, there is a need for certain GC (Government of Canada) stakeholders to be informed. These stakeholders may be internal to the GC (Government of Canada) CSEMP (Cyber Security Event Management Plan) governance structure, external to the GC (Government of Canada) CSEMP (Cyber Security Event Management Plan) structure but still within the GC (Government of Canada) (including intradepartmental or employee communications), or external (including media and the Canadian public). Continual (both routine and ad hoc) reporting and communication are vital in the cyber security event management process, ensuring that appropriate stakeholders at all levels of government are provided with the situational awareness required to make decisions and maintain an understanding of potential impact to GC (Government of Canada) programs and services.

This section will describe the reporting and communications products that will be distributed during the course of the GC (Government of Canada) event management life cycle, and the specific reporting requirements for departments and agencies.

5.1 Government-wide reporting and communication

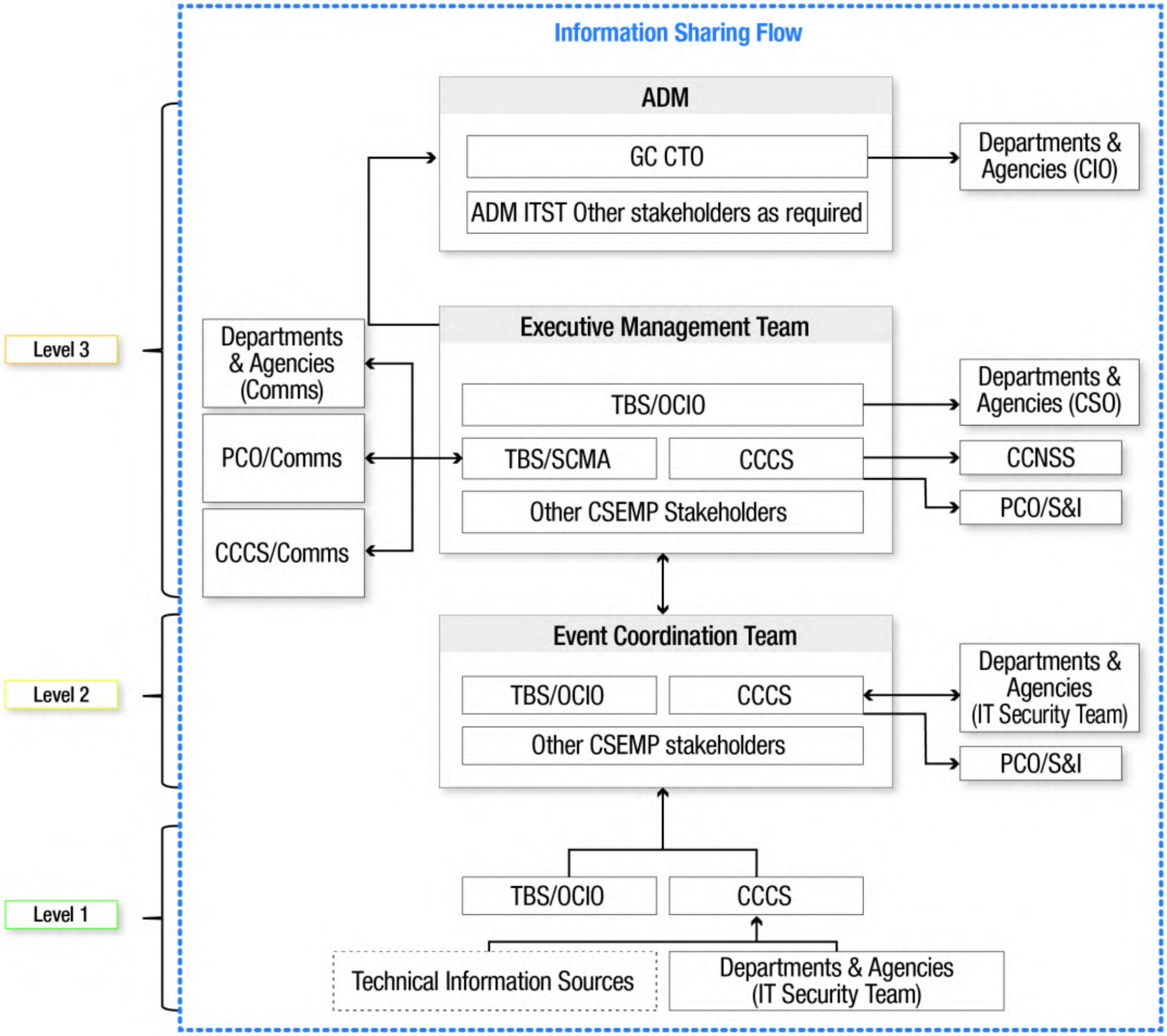
At the government-wide level, reporting and communication will be handled as follows:

- **TBS (Treasury Board of Canada Secretariat)-SCMA (Strategic Communications and Ministerial Affairs)** will coordinate the development of a communications strategy and develop and publish external communications materials (in accordance with TBS (Treasury Board of Canada Secretariat)'s Cyber Security Communications Framework [1]) required during the cyber security event management life cycle, in collaboration with CCCS (Canadian Centre for Cyber Security)-Comms (Communications) and PCO (Privy Council Office)-SC (Strategic communications) (for all events that require external communications or coordinated messaging)
- **affected departments and agencies** will develop their own stakeholder, client and public communications products (all events, but with TBS (Treasury Board of Canada Secretariat)-SCMA (Strategic Communications and Ministerial Affairs) and PCO (Privy Council Office)-SC (Strategic communications) approval for Level 3 and Level 4 events, in accordance with TBS (Treasury Board of Canada Secretariat)'s Cyber Security Communications Framework [1])
- **TBS (Treasury Board of Canada Secretariat)-OCIO (Office of the Chief Information Officer)** will coordinate messaging to the Chief Information Officer (CIO) and Chief Security Officer (CSO) community and disseminate Senior Management Updates as required throughout the cyber security event management process (Level 3 and Level 4 events or when situational awareness is required during Level 2 events)

- **CCCS (Canadian Centre for Cyber Security)-IMOC (Incident Management and Operational Coordination)** will communicate government-wide business impact assessment results with the GOC (Government Operations Centre) and Privy Council Office's Security and Intelligence (PCO (Privy Council Office)-S&I (Security and intelligence)) (Level 2 and Level 3 events)
- **GOC (Government Operations Centre)** will disseminate FERP (Federal Emergency Response Plan) governance updates and situational awareness products and briefings as required throughout the cyber security event management process (Level 3 and Level 4 events or when situational awareness is required during Level 2 events)
- **CCCS (Canadian Centre for Cyber Security)-IMOC** will coordinate messaging to the operational (IT (Information technology) Security) community and disseminate technical information products (cyber flashes, advisories, alerts, and so on), including GC (Government of Canada) CSEMP (Cyber Security Event Management Plan) response level status and situation reports to implicated stakeholders as required throughout the cyber security event management process (all events), in collaboration with TBS (Treasury Board of Canada Secretariat)-OCIO (Office of the Chief Information Officer) and other applicable partners
- **primary and specialized GC (Government of Canada) CSEMP (Cyber Security Event Management Plan) stakeholders** will ensure that appropriate organizations are notified when criminal-, terrorist- or military-related cyber event activity is detected (RCMP (Royal Canadian Mounted Police), CSIS (Canadian Security Intelligence Service) and DND respectively)
    - CCCS (Canadian Centre for Cyber Security)-IMOC (Incident Management and Operational Coordination) will take the lead on reporting to the RCMP (Royal Canadian Mounted Police), and to CSIS (Canadian Security Intelligence Service) or DND or both, if activity related to their mandates is discovered during the course of managing a GC (Government of Canada) event

A pictorial representation of the information-sharing flow can be found in Figure 6. Note that information-sharing at lower levels will continue in parallel to higher-level information-sharing.

Figure 6: CSEMP (Cyber Security Event Management Plan) Information-sharing flow


Information Sharing Flow
Level 3
Level 2
Level 1
ADM
GC CTO
ADM ITST Other stakeholders as required
Departments & Agencies (CIO)
Executive Management Team
TBS/OCIO
TBS/SCMA
CCCS
Other CSEMP Stakeholders
Departments & Agencies (CSO)
CCNSS
PCO/S&I
Departments & Agencies (Comms)
PCO/Comms
CCCS/Comms
Event Coordination Team
TBS/OCIO
CCCS
Other CSEMP stakeholders
Departments & Agencies (IT Security Team)
PCO/S&I
TBS/OCIO
CCCS
Technical Information Sources
Departments & Agencies (IT Security Team)

▼ Figure 6 - Text version

Figure 6 identifies the CSEMP information sharing flow separated by the different GC response levels outlined in figure two. Figure six applies only to the first three levels of response and does not address information sharing at Level 4 (emergency or crisis response).

1. Level 1 – Departmental response
    1. CCCS is the central agent in gathering information
    2. CCCS will obtain and provide information to the following sources:
        1. TBS-OCIO
        2. Departments and agencies (IT Security team)
        3. Technical information sources
    3. TBS-OCIO is to receive information only from CCCS
2. Level 2 – Limited GC-wide response
    1. The Event Coordination team is identified as the central source for information sharing
    2. The Event Coordination team is comprised of the following agents:
        1. TBS-OCIO
        2. CCCS
        3. other CSEMP stakeholders
    3. The Event Coordination team will provide and receive information from the following stakeholders:
        1. Departments and agencies (IT Security team) (through the CCCS)
        2. PCO-S&I (through CCCS)
        3. other CSEMP stakeholders
3. Level 3 – Comprehensive GC-wide response
    1. Two governance bodies are identified as central sources for information-sharing
    2. The first is the Executive Management team comprised of the following agents:
        1. TBS-OCIO
        2. TBS-SCMA
        3. CCCS
        4. other CSEMP stakeholders
    3. The Executive Management team (through TBS-OCIO) will provide information to departments and agencies (CSO)
    4. The EMT will provide and receive information from CCNSS as a committee

e. The EMT (through TBS-SCMA) will provide and receive information from Departments and Agencies (comms), PCO-Comms
f. The EMT (through TBS-OCIO) will inform the second level of governance at the ADM level
g. The second level of governance consists of:
    i. identified ADM committees
    ii. GC CTO
h. The GC CTO will provide information to departments and agencies at the CIO level

5.1.1 Reporting and communication summary

Below summarizes the types of reporting and communication that will occur internally in the GC (Government of Canada) over the course of a cyber security event under the GC (Government of Canada) CSEMP (Cyber Security Event Management Plan). Information-sharing between primary and specialized CSEMP (Cyber Security Event Management Plan) stakeholders will occur in accordance with established standard operating procedures. Note that this table does not describe day-to-day information-sharing that will continue through existing processes or mechanisms.

Table 1A: Reporting and communication summary between primary and specialized CSEMP (Cyber Security Event Management Plan) stakeholders

Type	Sender	Recipient	Timeline to issue
Situational awareness updates (for Level 2+ events)	**CCCS (Canadian Centre for Cyber Security)-IMOC (Incident Management and Operational Coordination)**	**TBS (Treasury Board of Canada Secretariat)-OCIO (Office of the Chief Information Officer)**	As new information becomes available (includes detection, mitigation and general status updates until event close-out)

Type	Sender	Recipient	Timeline to issue
Cyber security event reporting	**RCMP (Royal Canadian Mounted Police)** **CSIS (Canadian Security Intelligence Service)** **DND-CAF (National Defence/Canadian Armed Forces)**	**CCCS (Canadian Centre for Cyber Security)-IMOC (Incident Management and Operational Coordination)**	Upon detection of a malicious cyber security event related to GC (Government of Canada) systems
Mandate-specific reporting	**Primary and specialized GC (Government of Canada) CSEMP (Cyber Security Event Management Plan) stakeholders**	**RCMP (Royal Canadian Mounted Police)**	Immediately upon suspicion or detection of a cyber event related to criminal activity
		CSIS (Canadian Security Intelligence Service)	Immediately upon suspicion or detection of a cyber event related to terrorist activity
		DND	Immediately upon suspicion or detection of a cyber event related to national defence
Updates on impacts to the delivery of GC (Government of Canada) programs and services	**CCCS (Canadian Centre for Cyber Security)-IMOC (Incident Management and Operational Coordination)**	**PCO (Privy Council Office)-S&I (Security and intelligence)**	As new information becomes available

Type	Sender	Recipient	Timeline to issue
Situational awareness updates (for Level 2 events only)	**CCCS (Canadian Centre for Cyber Security)-IMOC (Incident Management and Operational Coordination)**	**GOC (Government Operations Centre)**	As new information becomes available (includes detection, mitigation and general status updates until event close-out)
External communications materials	**TBS (Treasury Board of Canada Secretariat)-SCMA (Strategic Communications and Ministerial Affairs)**	**Primary and specialized GC (Government of Canada) CSEMP (Cyber Security Event Management Plan) stakeholders**	As required

Table 1B: Reporting and communication summary from primary and specialized CSEMP (Cyber Security Event Management Plan) stakeholders to departments

Type	Sender	Recipient	Timeline to issue
Departmental incident notification	**CCCS (Canadian Centre for Cyber Security)-IMOC (Incident Management and Operational Coordination)**	**Affected department (ITSec (Information technology security) team)**	Immediately upon notification or detection of a malicious cyber security event

Type	Sender	Recipient	Timeline to issue
Cyber flashes, alerts, advisories	**CCCS (Canadian Centre for Cyber Security)-IMOC (Incident Management and Operational Coordination)**	**All departments (ITSec (Information technology security) team)**	**High+ Severity:** Within 8 hours of disclosure **Medium Severity:** Within 24 hours of disclosure **Low Severity:** Within 72 hours of disclosure
Requests for action (RFAs)	**CCCS (Canadian Centre for Cyber Security)-IMOC (Incident Management and Operational Coordination)**	**All departments (ITSec (Information technology security) team)**	As required (typically for high+ severity vulnerabilities when GC (Government of Canada)-wide exposure is unknown)
Technical situation reports	**CCCS (Canadian Centre for Cyber Security)-IMOC (Incident Management and Operational Coordination)**	**All departments (ITSec (Information technology security) team)**	**Level 2, 3 and 4 events:** As required
Senior management updates	**TBS (Treasury Board of Canada Secretariat)-OCIO (Office of the Chief Information Officer)**	**All departments (CIO (Chief Information Officer)s, CSO (Chief Security Officer)s)**	**Level 2, 3 and 4 events:** As required

Type	Sender	Recipient	Timeline to issue
GC (Government of Canada)-wide strategic direction to minimize impact of cyber event	**TBS (Treasury Board of Canada Secretariat)-OCIO (Office of the Chief Information Officer) (via GC (Government of Canada) CIO (Chief Information Officer))**	**All departments (CIO (Chief Information Officer)s)**	**Level 4 events:** As directed by FERP (Federal Emergency Response Plan) governance **Level 2 and 3 events:** As required
External communications materials	**TBS (Treasury Board of Canada Secretariat)-SCMA (Strategic Communications and Ministerial Affairs)**	**Affected department (Communications team)**	As required
All necessary information products	**CCCS (Canadian Centre for Cyber Security)-IMOC (Incident Management and Operational Coordination)**	**CCNSS (Canadian Committee on National Security Systems)**	As required

5.2 Departmental reporting requirements

5.2.1 Threat or vulnerability events

Mandatory departmental reporting on a threat or vulnerability event is required when an RFA (Request for Action) is issued by the CCCS (Canadian Centre for Cyber Security)-IMOC (Incident Management and Operational Coordination) (as described in subsection 4.2). Timelines for response will vary depending on the nature of the RFA; as such, each RFA will specify the target turnaround time for response. Response times specified will typically range from 24 to 48 hours, depending on the nature of the event.

RFA (Request for Action)s will always be sent to the generic departmental IT (Information technology) Security Operations mailbox. Departments need to ensure that this mailbox is monitored, with procedures in place to respond to these RFAs in a timely fashion.

5.2.2 Incidents

All cyber security incidents within the scope of this document (see subsection 2.3) will be reported to the CCCS (Canadian Centre for Cyber Security)-IMOC (Incident Management and Operational Coordination) in accordance with the Table 2. Reporting mechanisms and timelines for reporting will vary based on the departmental impact level, calculated by using the process outlined in Appendix B. CCCS (Canadian Centre for Cyber Security)-IMOC (Incident Management and Operational Coordination) will ensure appropriate storage of these incident reports and will share only information related to detection or mitigation techniques (for example, indicators of compromise, identification of malicious sites) with other departments and agencies. Sensitive department-specific information will not be shared GC (Government of Canada)-wide.

Table 2: Incident reporting requirements

Impact level	Initial incident report	Detailed incident report	Lessons learned report	Incident rollup summary
High or very high	**As soon as possible** after detection	Within 24 hours after detection	Within 30 days after resolution	Quarterly
Medium	Within 1 hour after detection	Within 48 hours after detection	Within 30 days after resolution	Quarterly
Low	n/a	n/a	n/a	Quarterly

5.2.3 Reporting examples

The CCCS (Canadian Centre for Cyber Security)-IMOC (Incident Management and Operational Coordination) is the central repository for cyber security event reporting in the GC (Government of Canada). While minor infractions may be dealt with at the departmental level, the majority of cyber security events must be reported to the CCCS (Canadian Centre for Cyber Security)-IMOC (Incident Management and Operational Coordination) in a timely fashion. The following examples, while not a complete list, can be used as a guide for types of events that should be reported:

- suspicious or targeted emails with attachments or links that were not detected by existing security controls
- suspicious or unauthorized network activity that represents a deviation from baseline
- data breaches or compromise or corruption of information
- intentional or accidental introduction of malware to a network
- denial-of-service attacks
- web or online presence defacement or compromise (including unauthorized use of GC (Government of Canada) social media accounts)

Consideration should also be given to whether events may impact other GC (Government of Canada) organizations. If in doubt, it is better to over-report than under-report.

5.2.4 Other

If there is reasonable evidence of suspected criminal activity under the *Criminal Code*, in addition to standard reporting to the CCCS (Canadian Centre for Cyber Security)-IMOC (Incident Management and Operational Coordination), departments and agencies will report **directly** to the RCMP (Royal Canadian Mounted Police) or Military Police, as applicable.

Departments will also report to the CCCS (Canadian Centre for Cyber Security)-IMOC (Incident Management and Operational Coordination) upon the realization that a cyber security event may require additional assistance in the mitigation and recovery phase (for example, aid from the CCCS (Canadian Centre for Cyber Security)-IMOC (Incident Management and Operational Coordination), RCMP (Royal Canadian Mounted Police), SSC (Shared Services Canada)-NSDS (Networks, Security and Digital Services), service providers) or if they are unable to implement given direction within the provided timeframe.

Departments and agencies providing services to other GC (Government of Canada) organizations are also responsible for notifying affected service recipients (in addition to their regular reporting to the CCCS (Canadian Centre for Cyber Security)-IMOC (Incident Management and Operational Coordination)) of any cyber security events that impact recipient information or service delivery.

Communications teams from affected departments and agencies will coordinate the development of stakeholder, client and public communications products with TBS (Treasury Board of Canada Secretariat)-SCMA (Strategic Communications and Ministerial Affairs), in accordance with the TBS (Treasury Board of Canada Secretariat)'s Cyber Security Communications Framework [1].

In the event of any real or suspected privacy breach, departments and agencies will respond in accordance with the *Directive on Privacy Practices*. Departments and agencies should apprise themselves of *TBS (Treasury Board of Canada Secretariat) Guidelines for Privacy Breaches* and the Privacy Breach Management Toolkit. These privacy instruments identify causes of privacy breaches, provide guidance on how to respond, contain and manage privacy breaches, delineate roles and responsibilities, and include links to relevant supporting documentation. Departments and agencies should consult legal counsel as needed.

5.3 Secure communications

During the cyber security event management life cycle (specifically, during the detection and assessment or mitigation and recovery phases), it frequently becomes necessary for key stakeholders to share information with one another. When this information becomes sensitive in nature (for example, specifics related to vulnerable IT (Information technology) systems, details about data exfiltration), secure communications methods must be used to transmit this information between stakeholders.

As such, all stakeholders need to be prepared to send and receive sensitive information. Such preparation includes ensuring that available secure communications tools (in other words, secure data and voice infrastructure) are in working order, with procedures in place and personnel trained for their use.

Stakeholders not equipped with sufficient tools will ensure that alternative manual processes are in place to send and receive this information, recognizing that these manual processes may delay receipt.

Appendix A: Roles and Responsibilities

▼ In this section

- 1. Primary GC (Government of Canada) Cyber Security Event Management stakeholders
- 2. Specialized GC (Government of Canada) Cyber Security Event Management stakeholders
- 3. Other stakeholders
- 4. Departments and agencies

This appendix describes roles and responsibilities of GC (Government of Canada) CSEMP (Cyber Security Event Management Plan) stakeholders. Roles and responsibilities will vary depending on the type of event (threat versus vulnerability versus security incident) and its priority level.

1. Primary GC (Government of Canada) Cyber Security Event Management stakeholders

The following is a list of primary stakeholders in the GC (Government of Canada) cyber security event management process that will be engaged in all events that meet the appropriate trigger criteria (including potential threats and vulnerabilities, and confirmed incidents). The degree of involvement from each stakeholder will vary based on the impact or severity of the event.

Treasury Board of Canada Secretariat

Treasury Board of Canada Secretariat (TBS) provides strategic oversight and direction in the GC (Government of Canada) cyber security event management process, ensuring that events are effectively coordinated in order to support decision-making and minimize potential impacts and losses to the GC (Government of Canada).

In the context of this plan, TBS (Treasury Board of Canada Secretariat)'s strategic oversight responsibilities, via its Office of the Chief Information Officer (OCIO), include:

- establishing, maintaining and testing the GC (Government of Canada) CSEMP (Cyber Security Event Management Plan) and related procedures
- ensuring strategic coordination of GC (Government of Canada) response to priority cyber security events (typically Level 3 events or, when warranted, by Level 2 events), which includes:
    - the role of co-chair and secretariat for all GC (Government of Canada) CSEMP (Cyber Security Event Management Plan) governance teams (including escalation and de-escalation decisions in coordination with CCCS (Canadian Centre for Cyber Security)-IMOC (Incident Management and Operational Coordination))
    - assessment of government-wide program and service impact of cyber threats, vulnerabilities and security incidents to support government-wide reporting and prioritization (assessed in collaboration with CCCS (Canadian Centre for Cyber Security)-IMOC (Incident Management and Operational Coordination) and other applicable partners)
    - issuance of direction (via the GC (Government of Canada) CIO) to departments and agencies on measures to minimize the GC (Government of Canada)-wide impact of significant cyber security events
- providing strategic advice to the Director General (DG) Event Response Committee (ERC) during Level 4 cyber security events
- ensuring that TBS (Treasury Board of Canada Secretariat)'s Strategic Communications and Ministerial Affairs (SCMA) team is provided with timely information required to develop communications products
- analyzing post-event reports from CCCS (Canadian Centre for Cyber Security)-IMOC (Incident Management and Operational Coordination) and conducting GC (Government of Canada)-wide lessons-learned exercises (when warranted) to drive security policy or enterprise security architecture related improvements

TBS (Treasury Board of Canada Secretariat)-SCMA (Strategic Communications and Ministerial Affairs) has a role in this plan regarding strategic communication, typically for Level 3 events (or when warranted by events at other levels). As the designated spokesperson on behalf of the GC (Government of Canada) for any cyber security event affecting government program and service delivery, TBS (Treasury Board of Canada Secretariat)-SCMA (Strategic Communications and Ministerial Affairs) is responsible for:

- developing internal (GC (Government of Canada)-wide) and external communications materials related to all phases of cyber security event management, in collaboration with the Communications Security Establishment's (CSE's) Communications and the Privy Council Office's (PCO (Privy Council Office)'s) Strategic Communications, and in consultation with communications teams from implicated CSEMP (Cyber Security Event Management Plan) stakeholders
- determining the necessity and timing of public statements (proactive and reactive)
- approving all communications plans (internal, stakeholder, client and public), in collaboration with affected organizations and PCO (Privy Council Office)'s Strategic Communications

Communications Security Establishment

Communications Security Establishment houses the Canadian Centre for Cyber Security (CCCS). It has several roles in relation to GC (Government of Canada) cyber security event management.

Coordination

Incident Management and Operational Coordination (IMOC) coordinates all operational phases of event management for cyber security events that have impacted or could impact the GC (Government of Canada). Coordination includes:

- monitoring the GC (Government of Canada) perimeter and all endpoints for which they have visibility, responding to cyber security events and implementing preventive and mitigation measures, as required

- acting as the central cyber operational contact in the GC (Government of Canada), both for distributing technical information products and for collecting event-related reports from GC (Government of Canada) organizations
- ensuring operational coordination of the GC (Government of Canada)'s response to all cyber security events, including:
  - monitoring technical information sources (including LSAs, affected departments and agencies, vendors) for precursors of cyber threat or vulnerability events or indicators of potential or confirmed cyber security incidents
  - issuing day-to-day security information products that contain technical advice for mitigating cyber threats (for example, alerts, advisories) and requests for action to departments and agencies
  - collating, tracking and reporting departments' reports on and responses to events and implementing technical mitigation measures
  - assessing the government-wide impact of cyber threats, vulnerabilities and security incidents on programs and services to support government-wide reporting and prioritization (assessed in collaboration with TBS (Treasury Board of Canada Secretariat)-OCIO (Office of the Chief Information Officer) and other applicable partners)
  - coordinating prevention, mitigation and recovery efforts, including providing timely situational awareness updates to other GC (Government of Canada) CSEMP (Cyber Security Event Management Plan) stakeholders
  - co-chairing all GC (Government of Canada) CSEMP (Cyber Security Event Management Plan) governance teams (including escalating and de-escalating decisions, in consultation with TBS (Treasury Board of Canada Secretariat))
- producing post-event reports that include a timeline of events and an analysis of root causes (based on departments' analyses and reports on lessons learned), and submitting them to TBS (Treasury Board of Canada Secretariat)-OCIO (Office of the Chief Information Officer) and other relevant organizations, as required (for example, PCO)
- communicating with TBS (Treasury Board of Canada Secretariat)-OCIO (Office of the Chief Information Officer) throughout the cyber security event management

life cycle
- verifying close-out of events and notifying appropriate CSEMP (Cyber Security Event Management Plan) stakeholders
- sharing cyber intelligence related to investigations and providing situational awareness related to cyber threats, vulnerabilities and attack techniques

Other services the CCCS (Canadian Centre for Cyber Security) offers to help departments and agencies recover from cyber security events and return to normal operations include but are not limited to:

- forensic examination and analysis (including evidence collection and investigation support)
- vulnerability analysis and response
- malware analysis and response

Usually, the CCCS (Canadian Centre for Cyber Security) manages delivery of these services, but prioritization may be recommended via the CSEMP (Cyber Security Event Management Plan) governance structure when warranted.

Technical advisory capacity

CCCS (Canadian Centre for Cyber Security) also develops, provides and operates capabilities and tools for managing cyber security events, and provides technical advice on the GC (Government of Canada) CSEMP (Cyber Security Event Management Plan). Its role in this involves:

- detecting, blocking or mitigating cyber threat activities that target GC (Government of Canada) networks or information
- providing reports and other information products to other key CSEMP (Cyber Security Event Management Plan) stakeholders
- supporting the identification, risk assessment, mitigation, recovery and post-analysis of cyber security events in the GC (Government of Canada)
- providing situational awareness of cyber security events (on GC (Government of Canada) systems that are Secret or below) to CCNSS (Canadian Committee on National Security Systems)

National coordination centre

CCCS (Canadian Centre for Cyber Security) is Canada's national coordination centre for preventing, mitigating, preparing for, responding to and recovering from cyber security events.

CCCS (Canadian Centre for Cyber Security)-Partnerships works with domestic and international partners to address significant cyber security concerns. Partners include critical infrastructure organizations and provincial, territorial and municipal governments. In the context of this plan, CCCS (Canadian Centre for Cyber Security) is responsible for sharing:

- cyber threat, vulnerability and incident information and warnings received from domestic and international partners with the GOC (Government Operations Centre)
- unclassified information from GC (Government of Canada) partners (threats, vulnerabilities, indicators, and so on) with domestic and international partners
- information on the potential scope and impact of a given event from the perspective of Canadian critical infrastructure owners and operators in order to ensure a comprehensive understanding of impacts that do not direct affect GC (Government of Canada) systems but that do affect the GC (Government of Canada) interest

Communications

During significant cyber events, CSE (Communications Security Establishment)'s Communications (Comms) team also plays a role. In the context of this plan, CSE (Communications Security Establishment)-Comms (Communications) is responsible for assisting TBS (Treasury Board of Canada Secretariat)-SCMA (Strategic Communications and Ministerial Affairs) by coordinating all federal public communications-related efforts during a cyber security event.

2. Specialized GC (Government of Canada) Cyber Security Event Management stakeholders

The following is a list of specialized stakeholders in the GC (Government of Canada) cyber security event management process that will be engaged for confirmed cyber security incidents or threat events that require specialized attention related to their particular mandates.

Shared Services Canada

Shared Services Canada (SSC) is responsible for the network infrastructure for 43 partners, for providing services to other GC (Government of Canada) departments and agencies and for managing the perimeter using gateways and secret infrastructure.

If a cyber security event occurs, SSC (Shared Services Canada) will coordinate with partners to determine whether any infrastructure it manages has to be shut down or be isolated from the network and will respond to recommendations from CCCS (Canadian Centre for Cyber Security)-IMOC (Incident Management and Operational Coordination) and direction from TBS (Treasury Board of Canada Secretariat)-OCIO (Office of the Chief Information Officer).

SSC (Shared Services Canada) also develops, provides and operates capabilities and tools for preventive defence of network infrastructure for the 43 partners. In the context of this plan, SSC (Shared Services Canada) is responsible for:

- blocking and mitigating cyber threat activities targeting SSC (Shared Services Canada)-managed networks or information
- responding to CCCS (Canadian Centre for Cyber Security)-IMOC (Incident Management and Operational Coordination) and TBS (Treasury Board of Canada Secretariat)-OCIO (Office of the Chief Information Officer) recommendations, and ensuring that updates and mitigating measures are applied in a timely manner
- implementing prevention, mitigation and recovery efforts, including timely situational awareness updates to key GC (Government of Canada) CSEMP (Cyber Security Event Management Plan) stakeholders
- providing reporting and other information products to key CSEMP (Cyber Security Event Management Plan) stakeholders
- supporting the identification, risk assessment, mitigation, recovery and post-analysis of cyber security events within the GC (Government of Canada)
- assessing government-wide program and service impact of cyber threats, vulnerabilities and security incidents to support government-wide reporting, to

be submitted to TBS (Treasury Board of Canada Secretariat)-OCIO (Office of the Chief Information Officer) and CCCS (Canadian Centre for Cyber Security)-IMOC (Incident Management and Operational Coordination)
- producing post-event reports, including timeline of events and root cause analysis and submitting to CCCS (Canadian Centre for Cyber Security)-IMOC (Incident Management and Operational Coordination), TBS (Treasury Board of Canada Secretariat)-OCIO (Office of the Chief Information Officer) and other relevant organizations, as required (for example, PCO (Privy Council Office))

Public Safety Canada

Public Safety Canada leads national cyber security policy and strategy by, for example, coordinating the overall response to significant national cyber events through the GOC (Government Operations Centre).

Royal Canadian Mounted Police

The Royal Canadian Mounted Police (RCMP) is the primary investigative department on all cyber security incidents dealing with actual or suspected cybercrime of non-state origin on the GC (Government of Canada) IT (Information technology) infrastructure.

In the context of this plan, the RCMP (Royal Canadian Mounted Police) is responsible for:

- leading the criminal investigation on cyber security incidents linked to non-state criminal activity (including criminal investigations involving terrorist activity)
- participating on GC (Government of Canada) CSEMP (Cyber Security Event Management Plan) governance teams in an advice and guidance capacity, when warranted by a particular cyber security incident or threat event

Canadian Security Intelligence Service

The Canadian Security Intelligence Service (CSIS) is the primary department responsible for investigating threats against information systems and critical infrastructure posed by foreign state actors and terrorists.

In the context of this plan, CSIS (Canadian Security Intelligence Service) is responsible for:

- leading the investigation on cyber security incidents that constitute a threat to the security of Canada, as defined by the CSIS (Canadian Security Intelligence Service) act (including terrorism and espionage)
- participating on GC (Government of Canada) CSEMP (Cyber Security Event Management Plan) governance teams in an advice and guidance capacity, when warranted by a particular cyber security incident or threat event

National Defence/Canadian Armed Forces

National Defence/Canadian Armed Forces (DND-CAF) is the primary department responsible for addressing cyber threats, vulnerabilities or security incidents against or on military systems. In the context of this plan, DND-CAF (National Defence/Canadian Armed Forces) is responsible for:

- leading the investigation on any cyber incidents (foreign or domestic) linked to activities directed against military systems (systems directly supporting military operational theatres and weapon systems)
- potentially providing additional support and assistance to other government departments, if tasked
- participating on GC (Government of Canada) CSEMP (Cyber Security Event Management Plan) governance teams in an advice and guidance capacity, when warranted by a particular cyber security incident or threat event

3. Other stakeholders

Government of Canada Chief Information Officer

The Government of Canada Chief Information Officer (GC CIO) represents whole-of-government interests during cyber security events that affect or may affect the delivery of programs and services, addressing topics that include overall GC (Government of Canada) response to cyber security events and enterprise-level actions taken to protect GC (Government of Canada) information systems. In the context of this plan, the GC (Government of Canada) CIO (Chief Information Officer) is responsible for:

- executing cyber security risk management decisions by acting on mandatory direction to departments in response to cyber security events (for example, implementing security controls and disconnecting systems that put the GC (Government of Canada) at risk, when warranted)
- briefing the Associate DM’s Office and higher as required in addition to advising Assistant Deputy Minister Committees on event-related issues, such as security and operations of GC (Government of Canada) IT (Information technology) systems and networks, service delivery and confidence in government
- chairing a committee of departmental CIO (Chief Information Officer)s through the CIO (Chief Information Officer) Council; through this Council, the GC (Government of Canada) CIO (Chief Information Officer) may issue direction to departmental CIO (Chief Information Officer)s regarding cyber security event management activities, specifically around mitigation and recovery related activities

Government Operations Centre

The Government Operations Centre (GOC), on behalf of the GC (Government of Canada), leads and supports response coordination of any type of event affecting the national interest; its role is not restricted to cyber events. It provides 24/7 monitoring and reporting, national-level situational awareness, warning products and integrated risk assessments, as well as national-level planning and whole-of-government response management. During periods of heightened response, the GOC (Government Operations Centre) is augmented by staff from other organizations (both government and non-government) that physically work in the GOC (Government Operations Centre) or connect to it virtually.

In the context of this plan, the GOC (Government Operations Centre) is responsible for:

- monitoring Level 3 cyber security events for potential escalation, which includes:
    - providing warning and situational awareness products to operations centres across government
    - conducting risk assessments and planning
    - briefing the FERP (Federal Emergency Response Plan) governance

- coordinating the overall GC (Government of Canada) response during Level 4 events, in accordance with the FERP (Federal Emergency Response Plan)

Privy Council Office

As the hub of non-partisan advice to the Prime Minister and Cabinet, PCO (Privy Council Office), in its role as a central agency, helps to clearly articulate and implement the GC (Government of Canada)'s policy agenda and to coordinate timely responses to issues facing the GC (Government of Canada) that are of national, intergovernmental and international importance. In that respect, PCO (Privy Council Office)'s Security and Intelligence (S&I) team has a leading role in the coordination of government-wide response to national security emergencies. In the context of this plan, PCO (Privy Council Office)-S&I (Security and intelligence) is responsible for:

- supporting the GC (Government of Canada) decision-making process by ensuring that senior officials are apprised in a timely manner of cyber security incidents that may be of national importance or may have national security implications
- participating on GC (Government of Canada) CSEMP (Cyber Security Event Management Plan) governance teams in an advice and guidance capacity, when warranted by a particular national incident or threat event

From a communications perspective, PCO (Privy Council Office)'s Strategic Communications (SC) team also plays a role during significant cyber events. In the context of this plan, PCO (Privy Council Office)-SC (Strategic communications) is responsible for providing communications advice to Cabinet and senior officials of the PCO (Privy Council Office) and coordinating government-wide communications, in collaboration with PS (Public Safety Canada)-Comms (Communications) and CSE (Communications Security Establishment)-Comms (Communications), including crisis management, during a cyber security event.

Canadian Committee on National Security Systems

The Canadian Committee on National Security Systems (CCNSS), chaired by CCCS (Canadian Centre for Cyber Security)'s Deputy Chief, develops and provides governance of an enterprise approach to securing those GC (Government of

Canada) systems requiring the highest level of assurance, known as National Security Systems. CCNSS (Canadian Committee on National Security Systems) leads a parallel EMP applying to all GC (Government of Canada) National Security Systems and can offer visibility to GC (Government of Canada) CSEMP (Cyber Security Event Management Plan) governance bodies on situations that may also impact non-National Security Systems. Such situations may also arise in the GC (Government of Canada) CSEMP (Cyber Security Event Management Plan) context; CCNSS (Canadian Committee on National Security Systems), therefore, benefits from a bidirectional triage bridge at the executive level and is a client of certain types of GC (Government of Canada) CSEMP (Cyber Security Event Management Plan) alerts.

Director General Event Response Committee

The Director General Event Response Committee (DG ERC) is a federal committee of directors general who manage operational response efforts and who direct, support and improve response planning and coordination for events affecting the national interest. In the context of this plan, the DG (Director General) ERC (Event Response Committee) becomes the GC (Government of Canada) CSEMP (Cyber Security Event Management Plan) interface into the FERP (Federal Emergency Response Plan) governance structure during Level 4 events, liaising with ADM (Assistant Deputy Minister), DM (Deputy Minister) and Cabinet Committees as required.

External partners

Departments and agencies often rely on various partners external to the GC (Government of Canada) to support program and service delivery, including private sector suppliers and other levels of government. External partners are required to manage and report on cyber events in accordance with the stipulations outlined in their respective contractual agreements with departmental service owners.

4. Departments and agencies

Departments and agencies play a key role in GC (Government of Canada)-wide cyber security event management, whether directly affected by an event or not. Detailed departmental roles and responsibilities related to security event management can be found in departmental governance, plans and procedures that are developed to support the implementation of the PGS (Policy on Government Security) and related directives and standards.

In the context of this plan, all departments and agencies are responsible for:

- reporting cyber security events as per section 5.2 of this plan
- monitoring CCCS (Canadian Centre for Cyber Security)-IMOC (Incident Management and Operational Coordination) technical information products and assessing their applicability to department-owned and -managed information systems
- assessing departmental program and service impact of cyber threats, vulnerabilities and security incidents
- responding to CCCS (Canadian Centre for Cyber Security)-IMOC (Incident Management and Operational Coordination) Requests for Action (RFAs) in accordance with specified timelines
- implementing mitigations based on direction and guidance issued by LSAs or central agencies
- notifying the CCCS (Canadian Centre for Cyber Security)-IMOC (Incident Management and Operational Coordination) if additional assistance is required to perform event response–related activities
- notifying appropriate law enforcement or national security authorities when an event falls under these domains
- participating on GC (Government of Canada) CSEMP (Cyber Security Event Management Plan) governance teams when requested by a co-chair (typically when affected by a cyber security event)
- following appropriate protocols upon occurrence of a privacy breach
- conducting post-event analysis and preparing departmental lessons-learned reports (for applicable events) and submitting them to the CCCS (Canadian Centre for Cyber Security)-IMOC (Incident Management and Operational Coordination)
- developing and disseminating applicable stakeholder and client management communications products (in consultation with or under the direction of TBS (Treasury Board of Canada Secretariat)-SCMA (Strategic Communications and

Ministerial Affairs) and PCO (Privy Council Office)-SC (Strategic communications), as required)
- ensuring that management and reporting requirements related to cyber security events are clearly stipulated in contracts, memoranda of understanding or other formal arrangements with external partners (for example, private sector suppliers and other levels of government) and that these address the requirements established in applicable GC (Government of Canada) and departmental policy instruments including, but not limited to, this plan
- developing, maintaining and testing departmental cyber security event management plans and processes, and ensuring alignment with GC (Government of Canada)-wide direction, plans and processes
- maintaining an up-to-date inventory of mission-critical information systems and understanding of information holdings in order to facilitate event response and prioritization
- continually maintaining and improving their departmental event response capability, including, but not limited to, implementing lessons learned (GC (Government of Canada)-wide and departmental), regularly exercising departmental plans and procedures, maintaining departmental contact lists, and training appropriate cyber security response personnel

Departments and agencies providing services to other GC (Government of Canada) organizations are responsible for establishing mechanisms to inform service recipients of cyber security events that impact their systems or information. Service providers are also responsible for providing service recipients with the information necessary to support GC (Government of Canada) CSEMP (Cyber Security Event Management Plan) reporting requirements outlined in subsection 5.2 of this plan (specifically, to support the completion of incident reports and responses to RFA (Request for Action)s) in a timely fashion, as well as any other digital evidence required to support departmental mitigation, recovery and post event activities.

Appendix B: Event Impact Assessment (Departmental)

▼ **In this section**

- Step 1 (for all cyber security events): Injury test
- Step 2 (for cyber threat and vulnerability events only): Risk assessment

The purpose of this appendix is to outline the high-level process used to assess impact related to a cyber security event. The end result of this process is the establishment of a departmental cyber security event impact level that will be used to determine an event response level for the GC (Government of Canada) as a whole.

Assessment of impact for all cyber security events (threats, vulnerabilities and confirmed incidents) begins with an injury test to measure the degree of injury that could reasonably be expected to occur due to a compromise (see Step 1). For confirmed cyber security incidents, the result of this injury test represents the departmental impact of the incident, as injury has been confirmed, and no further steps are required.

For cyber threat and vulnerability events, an additional step is required to determine the probability of injury occurrence in order to obtain a more accurate representation of potential departmental impact (see Step 2).

Step 1 (for all cyber security events): Injury test

The injury test, performed using Table 3, is based on severity and scope of the injury that could reasonably be expected to occur.

Severity: The severity of the injury refers to the level of harm, damage or loss (for example, from physical injury to loss of life, from minor financial losses to loss of financial viability, from minor inconvenience to significant hardship). The severity of the injury may be characterized as limited, serious or severe, based on an assessment of the following types of injury:

- harm to the health and safety of individuals
- financial losses or economic hardship
- impacts to government programs and services
- loss of civil order or national sovereignty

- damage to reputations or relationships

Other factors specific to a departmental or agency mandate or operational context may also be considered.

Scope: The scope of injury refers to the number of people, organizations, facilities or systems impacted, the geographical area affected (for example, localized or widespread), or duration of the injury (for example, short term or long term). The scope of injury can be characterized as:

- Wide: widespread; national or international; multiple countries or jurisdictions; major government programs or sectors
- Medium: jurisdiction, business sector, government program; group or community
- Narrow: individual, small business

Table 3: Injury test

		Scope		
		Narrow	**Medium**	**Wide**
Severity	**Severe**	Medium	High	Very high
	Serious	Low	Medium	High
	Limited	Low	Low	Medium
Departmental impact level		[Injury test result]		

Table 4 can be consulted to analyze potential expected results of a compromise and validate the outcome of the initial injury test. Once confirmed, this value can be entered in the incident report and submitted to the CCCS (Canadian Centre for Cyber Security)-IMOC (Incident Management and Operational Coordination).

Table 4: Expected results of compromise

Impact	**Result of compromise**

Impact	Result of compromise
Very high	- Widespread loss of life - Major long-term damage to the Canadian economy - Severe impediment to national security (e.g. compromising capabilities of Canadian Forces or national intelligence operations) - Severe damage to diplomatic or international relations - Long-term loss of public confidence in the GC (Government of Canada) that disrupts the stability of government
High	- Severe injury or loss of life to a group of individuals, or widespread serious injury - Serious financial loss that impedes the Canadian economy, compromises the viability of a GC (Government of Canada) program or reduces international competitiveness - Serious impediment to one or more mission-critical programs/services or impediment to national security - Serious damage to international relations that could result in a formal protest or sanction - Long-term loss of public confidence in the GC (Government of Canada) that disrupts a priority objective of the government
Medium	- Threat to the life or safety of an individual, or serious injury to a group of individuals - Financial loss that affects performance across a sector of the economy, affects GC (Government of Canada) program outcomes or affects the well-being of a large number of Canadians - Serious impediment to public-facing programs/services or departmental operations, jeopardizing program objectives - Damage to federal-provincial relations - Serious loss of public trust or confidence in the GC (Government of Canada) or embarrassment to the GC (Government of Canada)

Impact	Result of compromise
Low	• Physical or psychological harm to an individual • Financial stress or hardship to an individual • Impediment to departmental operations that could have a limited impact on program effectiveness • Harm to the reputation of an individual or business • Minor loss of public trust or confidence in the GC (Government of Canada)

Step 2 (for cyber threat and vulnerability events only): Risk assessment

Unlike cyber security incidents, where injury has been realized, injury is still in a potential state for cyber threat and vulnerability events. As such, in order to establish an accurate potential impact level, a risk assessment must be conducted (using Table 5) to determine the probability of occurrence for the injury. Using the results of the injury test performed in Step 1 (in other words, expected injury), a risk-modified departmental impact level is determined based on factors such as intelligence indicators (likelihood of compromise), exploitability, exposure of affected information systems, and implementation of compensating controls.

Table 5: Risk assessment

	Exposure			
	Low	Medium	High	Very high

		• Low likelihood that threat will target GC (Government of Canada) • Vulnerability very difficult to exploit • Vulnerable systems are not directly exposed (e.g. stand-alone systems) • Existing security controls effectively counter threat or vulnerability	• Medium likelihood that threat will target GC (Government of Canada) • Vulnerability exploitable with significant resources • Vulnerable systems are visible to one department only (for example, on its intranet) • Existing security controls partially counter threat or vulnerability	• High likelihood that threat will target GC (Government of Canada) • Vulnerability exploitable with moderate resources • Vulnerable systems are visible to many departments (for example, GC (Government of Canada) extranet) • Existing security controls provide limited protection against threat or vulnerability	• Threat or compromise imminent • Vulnerability easily exploitable with limited resources • Vulnerable systems are highly exposed (for example, Internet-facing) • Existing security controls do not provide protection against threat or vulnerability
Impact level (as per injury test in Step 1)	**Very high**	High	High	High	Very high
	High	Medium	Medium	High	High
	Medium	Low	Medium	Medium	Medium
	Low	Low	Low	Low	Low
Risk modified departmental impact level		[Risk assessment result]			

This risk-modified departmental impact level is to be reported to the CCCS (Canadian Centre for Cyber Security)-IMOC (Incident Management and Operational Coordination) (when requested via an RFA (Request for Action)) for consumption at the GC (Government of Canada)-wide level.

Cyber threat or vulnerability events are to be classified as cyber security incidents as soon as injury is realized. When injury moves from a potential state to a realized state, the injury tests in this appendix will require re-evaluation and resubmission to the CCCS (Canadian Centre for Cyber Security)-IMOC (Incident Management and Operational Coordination) to determine whether changes to event response or further escalation are required.

Appendix C: Response Level Calculation Matrix (GC (Government of Canada)-Wide)

Using the collated results of departmental impact assessments returned to the CCCS (Canadian Centre for Cyber Security)-IMOC (Incident Management and Operational Coordination), the GC (Government of Canada) response level is calculated based on the urgency of the cyber security event across the GC (Government of Canada) (using Table 6).

Table 6: GC (Government of Canada) response levels

	GC (Government of Canada) urgency		
	Low	**Medium**	**High**
	- Affects one internal GC (Government of Canada) program or service - Unlikely to propagate further	- Affects one external or several internal GC (Government of Canada) programs or services - Potential for broader propagation	- Affects multiple GC (Government of Canada) internal or external programs or services - Broader propagation imminent or confirmed

Departmental impact level (as per Appendix B)	**Very high**	Level 3	Level 3	Level 4
	High	Level 2	Level 2	Level 3
	Medium	Level 1	Level 2	Level 2
	Low	Level 1	Level 1	Level 1
GC (Government of Canada) response level		[Calculated GC (Government of Canada) response level]		

The GC (Government of Canada) response level calculation matrix is to be used as a guideline. There may be other externalities or escalating factors that need to be considered when establishing a GC (Government of Canada) response level. As such, TBS (Treasury Board of Canada Secretariat)-OCIO (Office of the Chief Information Officer) reserves the right to adjust the overall GC (Government of Canada) response level based on the context of any given cyber event scenario.

Footnotes

[1] Treasury Board of Canada Secretariat, "Communications Framework," 2015.

ISBN: 978-0-660-24005-3

Date modified:
2020-04-09