



Treasury Board of Canada  
Secretariat

Secrétariat du Conseil du Trésor  
du Canada

Canada

# Patch Management Guidance

Published: 2020-09-30

© Her Majesty the Queen in Right of Canada,  
represented by the President of the Treasury Board 2020,

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

Catalogue Number: BT39-60/2020E-PDF  
ISBN: 978-0-660-36866-5

This document is available on the Government of Canada website, [Canada.ca](https://www.canada.ca)

This document is available in alternative formats upon request.

Aussi offert en français sous le titre : Orientation sur la gestion des rustines

# Patch Management Guidance

---

From: [Treasury Board of Canada Secretariat](#)

## On this page

- [1. Introduction](#)
- [2. Patch management overview](#)
- [3. Patch management lifecycle](#)
- [4. Emergency patch management](#)
- [5. Operational environments](#)
- [6. Key performance indicators](#)
- [7. References](#)

## Introduction

### ► In this section

### Purpose and scope

The Treasury Board *Directive on Security Management* <sup>1</sup>, as part of Appendix B: Mandatory Procedures on IT Security Controls, requires departments to “Implement measures to protect information systems, their components and the information

they process and transmit against attacks that leverage vulnerabilities in information systems to affect their integrity and that could have an impact on their availability or confidentiality (for example, malicious code).” This includes implementing corrective actions such as applying patches to address vulnerabilities. In addition, the Canadian Centre for Cyber Security (CCCS) <sup>2</sup> prioritizes patching operating systems and applications as the second most important IT security action an organization can undertake to minimize intrusions and their impacts.

This document provides guidance on establishing an effective patch management strategy and identifies recommended key performance indicators (KPI) to measure in order to facilitate a continuous improvement approach.

The metrics in this guidance are recommended minimums and are provided to inform the evolution of an enterprise approach to patch management.

This guidance aligns with the following government artifacts:

- Policy on Government Security <sup>3</sup>
- Policy on Service and Digital <sup>4</sup>
- Directive on Security Management <sup>1</sup>
- Digital Operations Strategic Plan: 2018–2022 <sup>5</sup>
- Government of Canada Cyber Security Event Management Plan (GC CSEMP) <sup>6</sup>

## Target audience

This document targets IT service owners, IT service administrators and IT security operators responsible for acquiring, testing, prioritizing, deploying and verifying security patches throughout the federal government.

## Patch management overview

### ► In this section

Patches are modifications or updates made to firmware and software to correct functional and security deficiencies. Applying patches to operating systems,

applications and devices is a critical activity in ensuring the security of systems.

Patch management is a key organizational security control prescribed by CCCS's *IT Security Guidance*, ITSG-33 – System and Information Integrity Priority 1 Control (SI-2 Flaw Remediation) <sup>12</sup>.

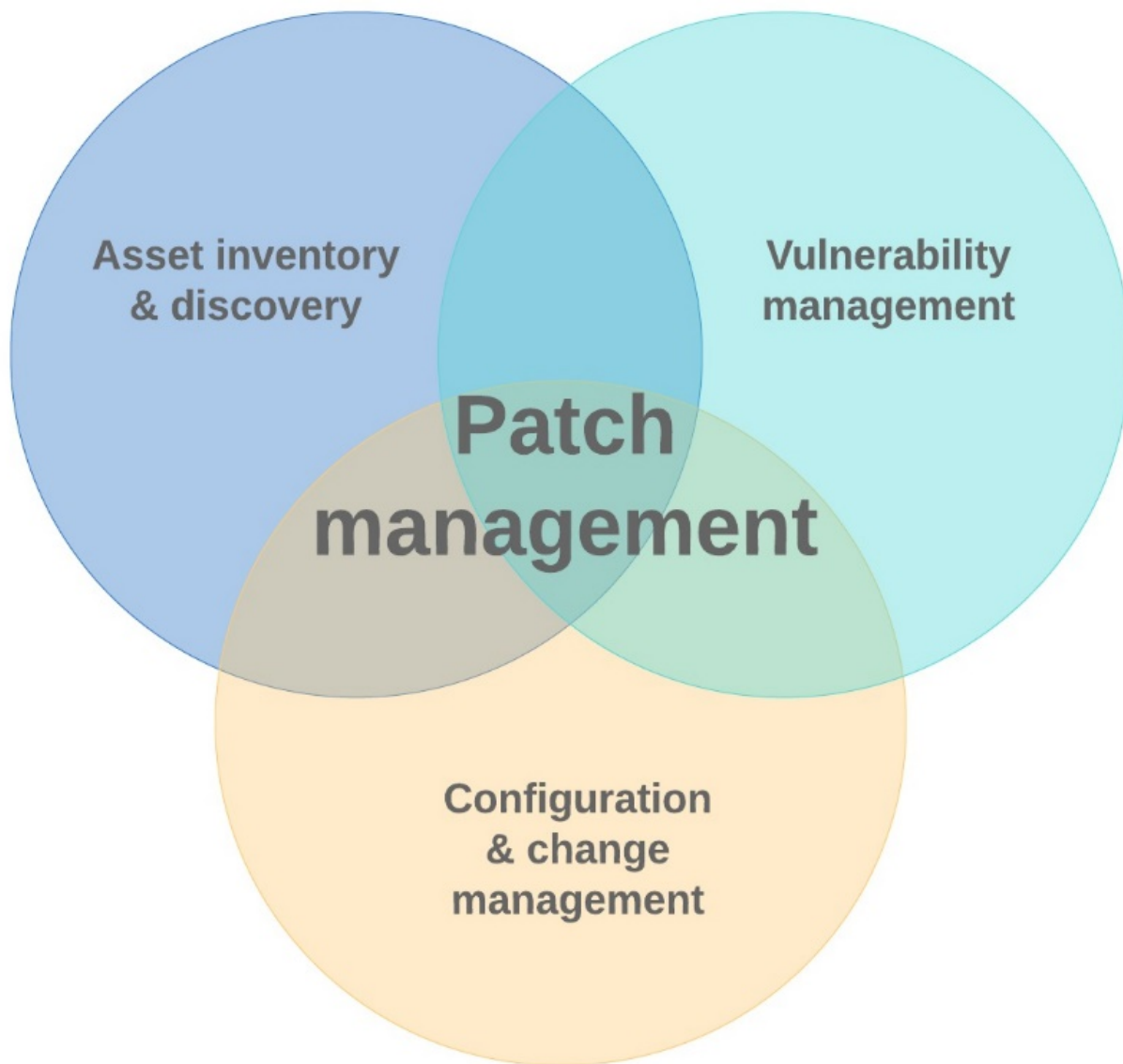
Patch management is the process for assessing, acquiring, testing, prioritizing, deploying and validating patches for products and systems <sup>7</sup>. Repeatable and standardized patch management activities support cost savings through the mitigation of software flaws and vulnerabilities, minimizing an organization's exposure and avoiding preventable compromises. Effective patch management requires coordination of various enterprise roles and processes to keep configurations up to date across heterogeneous IT environments. Security operators and service operators must work together to prioritize, test, apply and verify system and application patches while being mindful of operational requirements for availability.

## Patch management dependencies

A patch management process requires proper accountability and ownership, along with good governance and stewardship. Patch management is one of a number of components in a defence-in-depth strategy that should also include secure architecture design, integrated risk management, business continuity planning, and security operations functions such as monitoring and incident response.

The patch management process has foundational dependencies with three core operational capabilities, illustrated in Figure 2-1 Patch management foundational dependencies, which must be in place to ensure its efficiency and effectiveness.

### **Figure 2-1 Patch management foundational dependencies**



▼ Figure 2-1 - Text version

Figure 2-1 is a venn diagram that illustrates how the relationship between vulnerability management, configuration and change management, and asset inventory and discovery is a part of the whole patch management process.

### **Asset inventory and discovery**

Patch management requires a current and full inventory of an organization's software inventory, including versions and their disposition on networked hosts.

Common features of asset inventory and discovery, or asset management, intersect with vulnerability management and a broader patch management program. The asset inventory and discovery capability includes the identification of applications on assets, firmware on devices, versions and attributed vulnerabilities. It also provides remote management options, such as update, install, uninstall, and so on.

Attribution of assets to systems and the ability to reflect business criticality are premium features that can help inform decisions for patch prioritization and deployment timing, specifically the impact on service availability.

An asset management capability helps an organization track non-compliant software and firmware (such as expired versions) deployed in the IT environments. As a secondary benefit, it supports application rationalization, which allows for an inventory of “like” software in order to identify and eliminate redundant programs and unused licenses.

Asset inventory and discovery should include a continuous monitoring capability to automate the discovery of new network assets and also be integrated with the organization change and configuration management process/tool to ensure that prioritization for patching is always based on current asset information.

## **Vulnerability management**

Vulnerability scanning and vulnerability assessment (VA) are elements of vulnerability management and a foundational dependency for patch management. This dependency, from the perspective of the patch management process, intersects with asset inventory and discovery to correlate software inventories with identified vulnerabilities.

Automated scanning of networked systems using an enterprise VA capability provides the following benefits:

- Informs prioritization for patch deployment for commercial off-the-shelf (COTS) software.
- Helps establish and quantify the level of exposure and qualify the resultant risk from unmitigated vulnerabilities.

- Provides metrics concerning patch management performance over time, in turn allowing the organization to mature the efficiency and effectiveness of their patch management program.

For detailed information regarding the technology options and capabilities of vulnerability management platforms, it is recommended to review NIST publication SP 800-40 Rev. 3, *Guide to Enterprise Patch Management Technologies* [\[7\]](#). This guidance, originally published in 2013, establishes a solid foundation for understanding the function of vulnerability management tools; however, the domain has since evolved and supplemental research is recommended to become current on the options and capabilities of modern platforms.

A continuous monitoring capability to automate vulnerability assessment should be a function of the vulnerability management platform. Implementing this capability is a best practice to ensure that prioritization for patching is always based on current risk information. While outside of the scope of this guidance, it is worth noting that cyber event and incident management also rely on up-to-date vulnerability management data to accurately assess the potential or actual impacts of an incident.

Commercial vulnerability management platforms typically cannot detect flaws in custom business applications or government off-the-shelf (GOTS) applications. The risk-managed lifecycle of these categories of applications should include periodic targeted vulnerability assessment to identify software flaws and configuration deficiencies.

Custom applications often rely on underlying COTS or open-source components, packages or frameworks. Application owners must be aware of these dependencies and of their responsibilities towards patch management versus those of service providers. Direction for how to address these circumstances should be addressed in the patch management process.

## **Configuration and change management**

Patching of software is a configuration change and should be accounted for in a configuration and change management process. Patches and updates must be



tracked through the departmental change management system. Patch application plans submitted through change management must have associated contingency and rollback plans (see the **Validation** phase of the patch management lifecycle for more details).

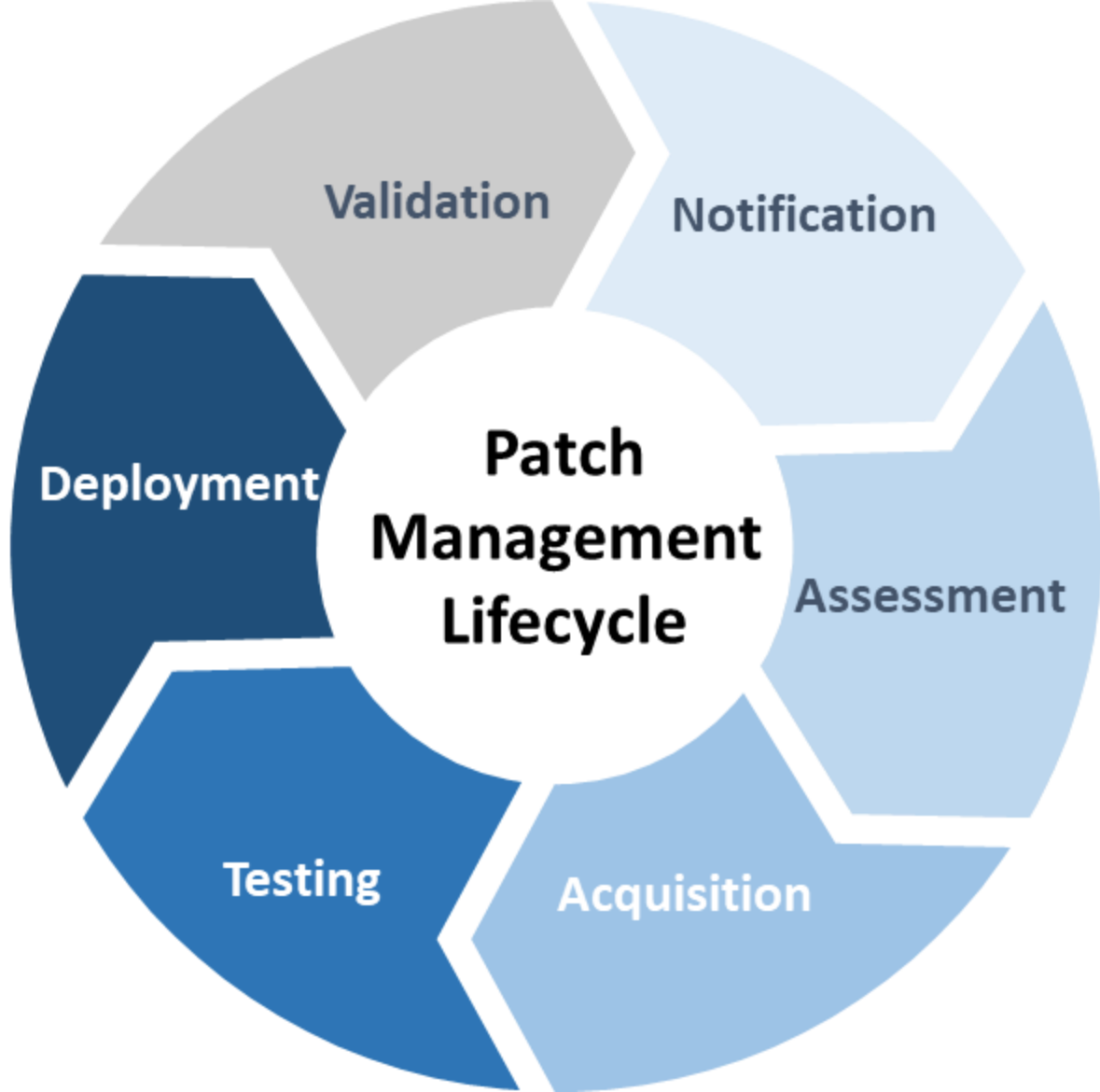
Platforms and applications should be deployed in a hardened configuration, according to CCCS's Top 10 guidance [2](#). Features that are enabled by default but that are not required for processing should be disabled to minimize exposure and reduce the urgency for emergency patch measures (see the **Assessment** phase of the lifecycle for more details).

## Patch management lifecycle

### ► In this section

Patch management is a closed-loop process that is part of an organization's overall system integrity and risk management strategy. The process is best executed when it is repeatable and largely automated through an enterprise tool that incorporates the foundations of vulnerability management and asset inventory and discovery. The tool facilitates a continuous monitoring capability and executes the cyclical process as described in the sections that follow.

### **Figure 3-1 Patch management lifecycle**



▼ Figure 3-1 - Text version

Figure 3-1 is a cycle diagram that shows the six stages of the patch management lifecycle: notification, assessment, acquisition, testing, deployment, and validation. Each stage is then described in detail in the sections that follow.

## Notification

Triggers for the patch management process might include vulnerability notifications from:

- Enterprise patch management software: The software maintains an application inventory and patch definition database, notifying administrators when new updates are published and downloaded from trusted sources.

- Mobile device management: A platform for managing mobile devices such as tablets and smartphones will include notifications and policies for remotely updating device apps.
- CCCS publications: Alerts and advisories from CCCS are available via RSS and listed on their website [8](#). CCCS publications are also sent to each GC organization's generic departmental IT Security Operations mailbox, from which they can be forwarded to team mailboxes or individual operational staff.
- Vendor notification: Individual vendors typically offer a subscription service for notification of patches and updates.
- Internal operational processes: An organization can trigger the patch management process as a result of internal operational processes, most often those associated with security, such as resulting from an incident, resulting from a VA.
- Other: Media reports, social media, cyber security companies, vulnerability aggregator services, mailing lists, RSS feeds, and so on.

GC organizations are **required** to maintain a generic IT Security Operations mailbox according to the GC CSEMP [6](#). The ITSG-33 controls profile also requires compliance for monitoring for and receiving CCCS security publications. (See System and Information Integrity control SI-5 (Security Alerts, Advisories, and Directives) [12](#).)

## Assessment

The severity rating that the vendor or developer has assigned to a patch is a prime indicator of its importance and of the priority it should be given; however, patch prioritization in the GC is also a risk assessment activity that considers the risk that a vulnerability represents in the context of the operating environment.

CSE's *ITSB-96 – Security Vulnerabilities and Patches Explained* [9](#) identifies the factors that should be considered by GC departments when determining the priority for a patch, including its potential impact on high-valued assets, threat profile, exploit

complexity and likelihood, and the impact of mitigating controls on its exposure. This CCCS guidance should be consulted and referenced when crafting a departmental assessment framework for patch priority.

### Deployment schedule

Once priority has been assessed, a determination on a deployment time frame must be made. While a patch that addresses functionality might have a deployment schedule based solely on a concern with minimizing the impact to business, a security patch, by default, must be set at a higher priority. CCCS's *ITSB-96* <sup>9</sup> also provides guidance regarding deployment time frames for security patches in the GC and their recommendations are summarized in the following table:

**Table 3-1 CCCS suggested deployment schedule**

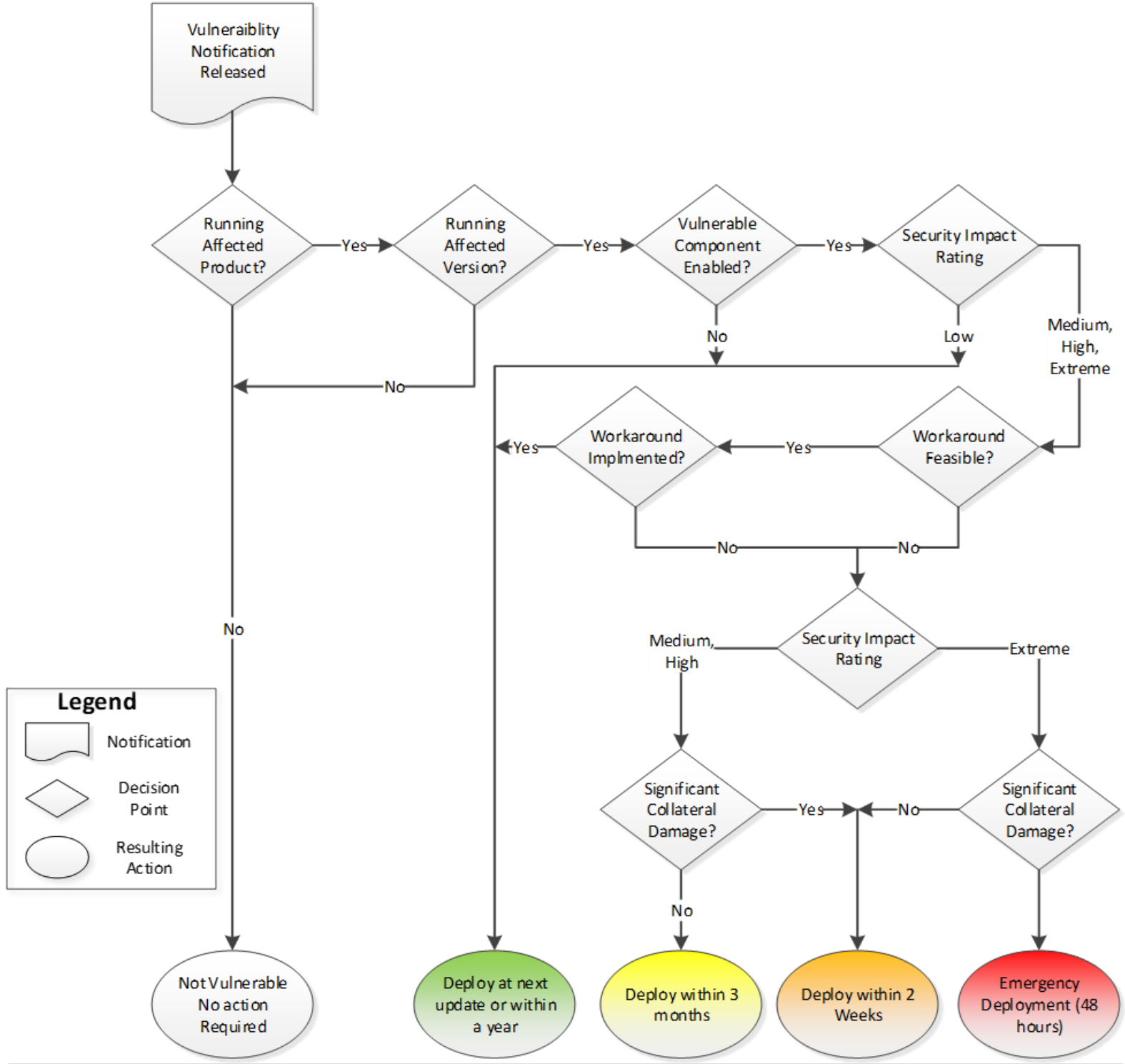
| Patch priority | Suggested deployment schedule                  |
|----------------|--|
| Extreme        | Emergency: Deploy within 48 hours              |
| High           | Deploy within 2 weeks                          |
| Medium         | Deploy at next major update or within 3 months |
| Low            | Deploy at next major update or within 1 year   |

CCCS's deployment schedule only suggests timelines for deployment. In actuality, an organization should take into consideration risk tolerance and exposure to a given vulnerability and associated attack vector(s) as part of a risk-based approach to patching, while also fully considering their individual threat profile. Patch management tools continue to improve the efficiency of the process and enable organizations to hasten the deployment schedule.

As a general rule, GC organizations should always prioritize critical systems and services in any patching scenario. Critical systems and services are defined by TBS as "those whose compromise in terms of availability or integrity would result in a high degree of injury to the health, safety, security or economic well-being of Canadians or to the effective functioning of the GC" <sup>3</sup>.

Figure 3-2 illustrates the steps and rationale for arriving at the correct patch priority and corresponding deployment schedule. When employed, the process must also take into consideration the unique conditions of each situation and the factors listed in the **Assessment** section, including but not limited to existing workarounds or mitigating controls, threat profiles and vulnerability details, and potential for collateral damage, specifically to critical assets and services.

**Figure 3-2 Vulnerability impact and patch deployment schedule flowchart**



▼ Figure 3-2 - Text version

Figure 3-2 presents a flowchart for determining the actions to take in response to a vulnerability notification. The steps are as follows:

- After receipt of a notification, the organization determines whether they have deployed the affected product and version(s), and if the vulnerable components of the software are enabled. If the software is deployed but the vulnerable component(s) are not enabled, a patch may be deployed at the next update or within the year.
- If the vulnerable component(s) are enabled, the organization then determines whether the security impact is low, medium, high, or extreme.
- A low impact vulnerability may be addressed at the next update or within the year. All other ratings require the organization to continue with the process to determine whether a workaround to mitigate the vulnerability exists and is implemented.
- If the answer is yes, the update can be deployed at the next update or within the year. If a mitigation is not in place, the security impact rating is used to determine the next course of action.
- For medium and high impact vulnerabilities without a chance of significant collateral damage, deployment of an update may occur within three months.
- For medium or high impact vulnerabilities that could incur significant collateral damage, for example by exposing additional assets to risk of compromise, patch deployment should occur within two weeks.
- If a vulnerability impact is determined to be extreme but without risk of significant collateral damage, the two-week window for patch deployment also applies.
- For extreme impact vulnerabilities that also include a risk of significant collateral damage to other assets, an emergency deployment schedule of patching within 48 hours of notification applies.

Patches are commonly acquired from the software vendor or other trusted source, for example community software development or standard Linux repositories. Enterprise patch management software can automate the download and verification of patches, typically using verification methods that are based on integrity checksums and digital signatures.

If a patch is obtained via manual download, the source and integrity of the package must be confirmed prior to its deployment.

## **Testing**

Patch testing can be carried out in a test or sandbox network that simulates the production environment. While this is the ideal approach, it is also the most expensive and impractical. Virtualization can be used to minimize hardware costs and capitalize on deploying a wide array of systems in a test environment, but it will not address the overall overhead of maintaining a parallel environment.

The recommended alternative is to leverage a community of users across all business units of the organization as a production test bed for patch deployment. Feedback regarding faults can be used to determine whether there is an operational impact to deploying a patch. That impact must then be measured against the risk of delaying deployment or not patching and resorting to a workaround.

Workarounds are temporary fixes, such as disabling the vulnerable functionality or implementing access controls to limit its exposure. They can be considered if faults are identified and waiting for an operable patch is not a viable option due to heightened risk.

Patches can be tested individually or alternatively bundled to ensure that faults are detected prior to wide-scale deployment.

## **Deployment**

Enterprise patch management software is the preferred method for distribution of software updates. Patches can be bundled or applied incrementally and should be

staggered across the enterprise to ensure that a service outage does not occur if a fault materializes that was not revealed during the testing phase.

Auto-update is a feature common for many applications but generally not recommended for an enterprise environment given that its use removes patch testing, beyond that performed by the vendor, from the process. That said, there are situations where auto-update may be the preferred deployment method, for example in the case of web browsers and mobile apps. Other scenarios may apply and GC organizations must perform their own risk management due diligence when deciding whether and where to enable auto-update functionality.

Note also that enterprise deployment may not be feasible in all instances, such as in the case of GOTS or custom applications, and alternative deployment options such as scripted or manual patch application should be accounted for in an organization's patch management strategy to address outliers and exceptions.

## **Validation**

An audit of patch deployment success and failure rates should be performed after each deployment to identify outliers, and to trace and correct patch installation failures. The asset inventory and discovery features of an enterprise patch management suite will reflect the status of the deployment and provide the statistics to satisfy KPI and Service Level Agreement requirements defined in the organization's strategy.

Execution of a rollback process may be required if a patch deployment results in unexpected impacts on production systems. Insights gained from investigation and correction of installation failures should be used to augment the patch management program and minimize the need for similar rollback and corrective activity in the future.

## **Emergency patch management**

The circumstances for declaring an emergency patch situation will differ and depend heavily on the assets, firmware, operating systems and applications deployed in an



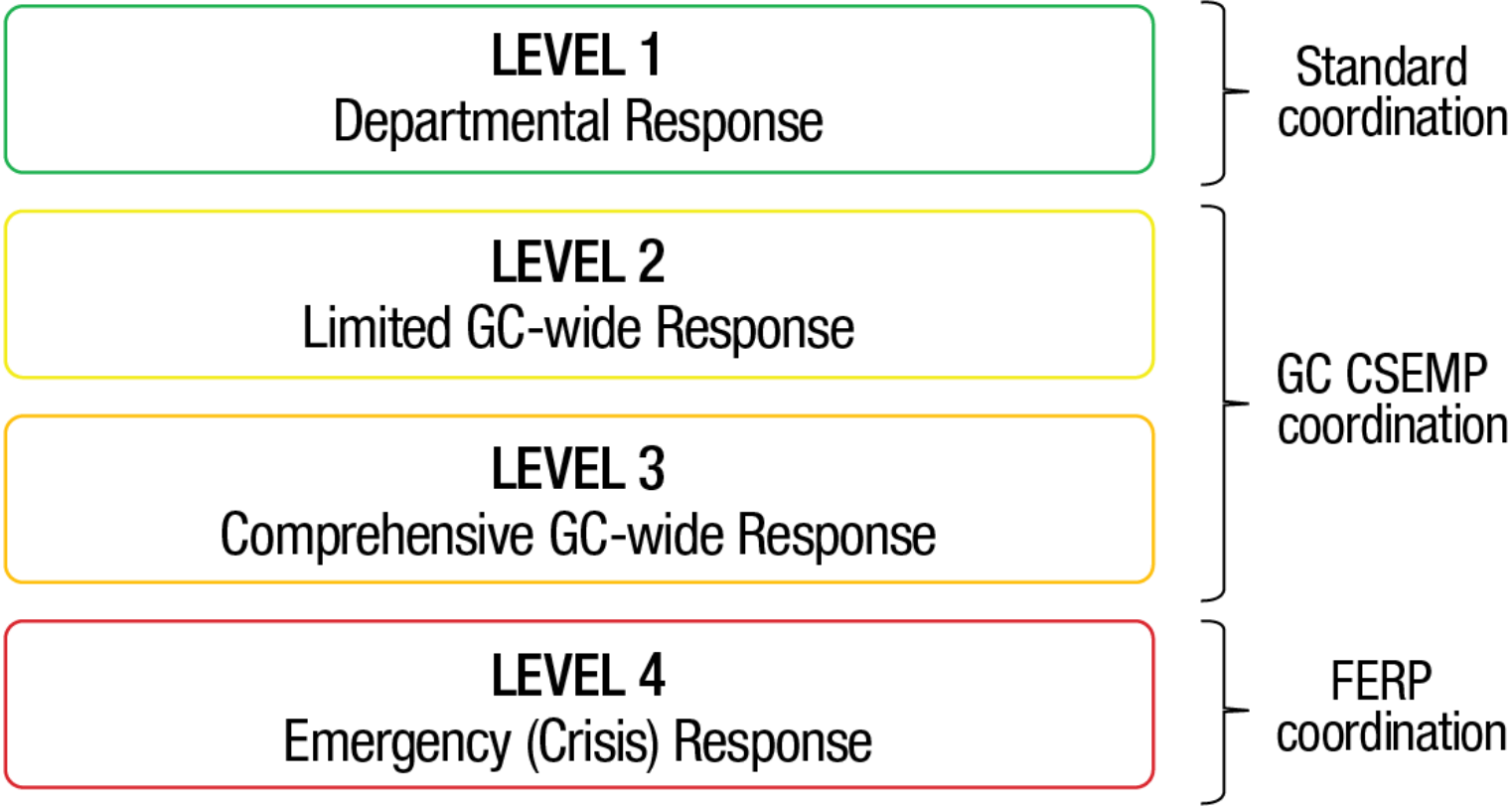
organization's infrastructure. The decision to immediately deploy a critical patch should be based in risk management, as outlined in section 3.2.1 Deployment schedule.

In the context of a government-wide emergency patch management scenario, the *GC Cyber Security Event Management Plan* <sup>3</sup> outlines the stakeholders and actions required to ensure that cyber security events are addressed in a consistent, coordinated and timely fashion. Cyber security events include vulnerability notifications that may require GC organizations to execute emergency patch management procedures.

This scenario is initiated in the **Notification** phase of the patch management lifecycle with the release of a *Cyber Flash* publication by the CCCS.

The decision to issue a *Cyber Flash* is made by the Lead Security Agencies (LSA) and Specialized LSA Stakeholders and may be taken for a Level 2 or Level 3 CSEMP event (see GC CSEMP <sup>6</sup> for detailed information concerning CSEMP levels).

**Figure 4-1 GC CSEMP response levels**



▼ Figure 4-1 - Text version

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

A *Cyber Flash* is commonly issued when a critical vulnerability applies to a product and version that is ubiquitous in the GC, has an extreme exploit impact, is unlikely to be protected against by mitigating controls, and can result in significant collateral damage to critical systems or services.

After the receipt of a *Cyber Flash*, GC organizations are required to perform an impact assessment to determine their exposure to and the potential impact from the vulnerability's compromise. Emergency patching should result if the potential security impact is *extreme* with probable significant collateral damage in line with the LSA's assessment.

When an emergency deployment is declared, the remaining phases of the lifecycle remain largely unchanged; however, the time frame for **Testing** and **Deployment** must be streamlined to align with the urgency of mitigating the vulnerability.

Lastly, the **Validation** phase may require providing feedback to the CCCS regarding the progress or completion of the remediation effort.

## Operational environments

## ► In this section

The following subsections briefly describe the operational environments most commonly encountered in the GC. This list is not exhaustive or authoritative, and it does not cover all of the potential operating conditions for GC systems. The role and responsibilities ascribed to the change management process, both outside and inside an organization, will ultimately be unique, take into consideration the organization's dependence on external service providers, and may rely on contract vehicles, contract authorities and/or memorandums of understanding.

### **Organizational infrastructure**

GC departments and agencies are the authority for their own IT infrastructure and are responsible for implementing tools and processes to meet standard timelines for remediation and for ensuring quick response times for emergency or critical patch deployment [1](#). For organizations that operate autonomously, this infrastructure might include servers, network equipment, workstations, applications, and so on. For those under the purview of Shared Service Canada (SSC), it would be a subset of the above.

### **Shared Services Canada**

SSC acts as service provider for GC departments and has developed its own *Patch Management Standard* which defines the stages and steps, and the roles and responsibilities for effective patch management of SSC infrastructure in enterprise data centres and legacy client networks [10](#).

SSC's responsibilities do not extend to the organizational infrastructure referenced above. As such, the departments serviced by SSC are required to coordinate change and configuration management activities with SSC, including all patch management activities, in order to ensure proper testing, prioritization, deployment and validation.

### **Cloud service providers and managed service providers**

The *GC Cloud Adoption Strategy* prescribes a “cloud-first” approach in which cloud is the preferred option for delivering IT services in the GC [11](#). Cloud service providers may be leveraged to deliver one or more of the defined cloud service models of Infrastructure as a Service, Platform as a Service and Software as a Service.

GC cloud consumers who leverage a cloud service provider or other value-add third party, such as a managed service provider, must account for patch management and emergency patch management in their contracts.

## Key performance indicators

A patch management strategy should include measures for KPIs in order to evaluate its effectiveness and efficiency. An enterprise patch management system should provide reporting capabilities to allow for this measuring over time. Some examples of KPIs include:

- Coverage:
  - The percentage of systems and applications within the organization inventoried and covered by automated patch management
- Efficiency and effectiveness:
  - How often hosts are automatically checked for compliance
  - How often asset inventories are automatically updated
  - The minimum/average/max time to patch X percentage of hosts
  - The percentage of systems patched within X, Y, Z days after deployment
  - The percentage of operational hosts within the organization fully patched at any given time
  - The number of extreme impact, high impact, medium impact, low impact hosts and/or unpatched vulnerabilities on organizational hosts at any given time
  - Average time elapsed between a patch’s availability and its production implementation per level of rating
  - The percentage of hosts patched automatically vs. partially (in the case of patches bundled in a package) vs. manually

- The percentage of patches deployed within the suggested deployment schedule

Regular reporting on KPIs will enable the organization to establish a baseline of the performance of their patch management process and to quickly mature it.


---

## 7. References

- 1 Treasury Board of Canada Secretariat, [Directive on Security Management](#).
- 2 Canadian Centre for Cyber Security, [Top 10 IT Security Actions to Protect Government of Canada Internet-Connected Networks and Information \(ITSB-89 v3\)](#).
- 3 Treasury Board of Canada Secretariat, [Policy on Government Security](#).
- 4 Treasury Board of Canada Secretariat, [Policy on Service and Digital](#).
- 5 Government of Canada, [Digital Operations Strategic Plan](#).
- 6 Government of Canada, [Government of Canada Cyber Security Event Management Plan](#).
- 7 National Institute of Standards and Technology, [Guide to Enterprise Patch Management Technologies SP 800-40 Rev. 3](#), 2013.
- 8 Canadian Centre for Cyber Security, [Alerts & Advisories](#).
- 9 Canadian Centre for Cyber Security, [Security Vulnerabilities and Patches Explained - IT Security Bulletin for the Government of Canada \(ITSB-96\)](#).
- 10 Shared Services Canada, «Shared Services Canada Patch Management Standard» April 2019.
- 11 [Government of Canada Cloud Adoption Strategy: 2018 update](#).

[▶ Report a problem or mistake on this page](#)[↻ Share this page](#)

Date modified: 2020-09-30

[Contact us](#)[Departments and agencies](#)[Public service and military](#)[News](#)[Treaties, laws and regulations](#)[Government-wide reporting](#)[Prime Minister](#)[About government](#)[Open government](#)[• Social media](#)[• Mobile applications](#)[• About Canada.ca](#)[• Terms and conditions](#)[• Privacy](#)[Top of page](#) The logo for the Government of Canada, featuring the word "Canada" in a serif font with a stylized red maple leaf above the letter 'a'.