Communications Security Establishment
Centre de la sécurité des télécommunications

CANADIAN CENTRE FOR CYBER SECURITY

Top 10 IT security actions: No. 2 patch operating systems and applications

MANAGEMENT

Foreword

This document is an unclassified publication that is part of a suite of documents that focus on each of the top 10 IT security actions recommended in *ITSM.10.089 Top 10 Information Technology Security Actions to Protect Internet-Connected Networks and Information* [1][1].

Effective date

This publication takes effect on August 5, 2022.

Revision history

Revision	Amendments	Date
1	First release.	August 5, 2022

[1] Numbers in square brackets refer to a reference cited in the Supporting Content section of this document.

Overview

One of our top 10 recommended IT security actions is to patch operating systems and applications. This document outlines several best practices for patching. The guidance in this document is based on the security controls found in *ITSG-33 IT Security Risk Management: A Lifecycle Approach* [2].

Software vendors discover and disclose vulnerabilities in their software and release new patches to address problems. However, by disclosing vulnerabilities to the public, software vendors are also providing threat actors with knowledge on current vulnerabilities. Your organization, regardless of its size, is a target for threat actors. If you don’t take the steps to test, manage changes, and deploy software patches as soon as they are released, threat actors can use software vulnerabilities to exploit your networks, systems, and IT assets.

This document is part of a suite of documents that focuses on the top 10 IT security actions recommended in ITSM.10.089 [1]. While implementing all 10 of the recommended security actions can reduce your organization’s vulnerability to cyber threats, you should review your current cyber security activities to determine whether additional actions are required. For more information on implementing the top 10 IT security actions, email, or phone our Contact Centre:

Contact Centre
contact@cyber.gc.ca
(613) 949-7048 or 1-833-CYBER-88

Table of contents

List of figures

List of tables

List of annexes

1 Introduction

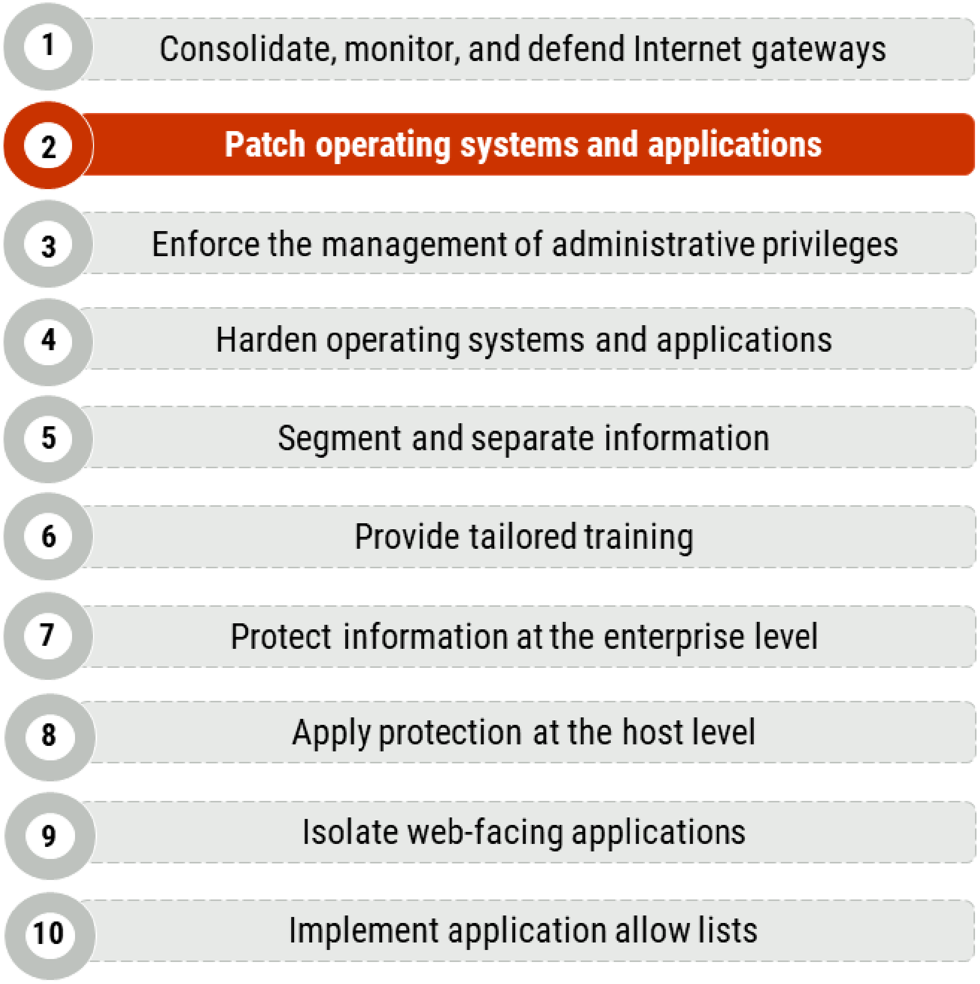
This document provides guidance on best practices when performing patching to your operating systems (OS) and applications. Patching, which includes the actions to test, manage changes, and implement updates and patches, reduces your organization's exposure to threats that could exploit publicly known vulnerabilities and compromise your networks, systems, and IT assets. This guidance is based on the advice in ITSM.10.089 [1] and the security controls listed in Annex 3A of ITSG-33 [2].

1.1 Top 10 IT security actions

Our top 10 recommended IT security actions, which are listed in Figure 1 below, are based on our analysis of trends in cyber security threat activities and the impact of those threat activities on Internet-connected networks. The top 10 includes prioritized security actions that your organization should take as a baseline to strengthen its IT infrastructure and protect its networks. Although we recommend following the numerical order of these actions (starting with #1) to increase your protection efforts against cyber threats, you can change the sequence of actions to meet your organization's needs and requirements. As you add security actions to your environment, your threat surface (all available endpoints that a threat actor may try to exploit) decreases, and your security posture increases.

Keep in mind that these actions are just a starting point, and there is no single strategy that is guaranteed to prevent cyber incidents. The cyber threat landscape continues to evolve, and you should ensure that you reassess your risks and review your current security efforts to address any gaps or weaknesses.

When determining your security needs, you should also consider whether your organization will use an on-premises model or outsource to a cloud service provider (CSP) or a managed service provider (MSP). If you decide to work with a CSP or MSP, you should assess the threats, vulnerabilities, shared responsibilities, and cloud platform capabilities so that you can implement appropriate security controls. The ways in which you follow the top 10 may differ depending on the types of services you are using. For example, the roles and responsibilities of your organization and your CSP or MSP will vary depending on the services you are consuming, your service model, and your deployment model. However, even when using cloud or managed services, your organization is still legally responsible and accountable for securing its data. For more information on security and cloud or managed services, see *ITSM.50.062 Cloud Security Risk Management* [3] and *ITSM.50.030 Cyber Security Considerations for Consumers of Managed Services* [4].



1. Consolidate, monitor, and defend Internet gateways
2. Patch operating systems and applications
3. Enforce the management of administrative privileges
4. Harden operating systems and applications
5. Segment and separate information
6. Provide tailored training
7. Protect information at the enterprise level
8. Apply protection at the host level
9. Isolate web-facing applications
10. Implement application allow lists

Figure 1: Top 10 IT Security Actions - #2 Patch operating systems and applications

1.2 IT security risk management process

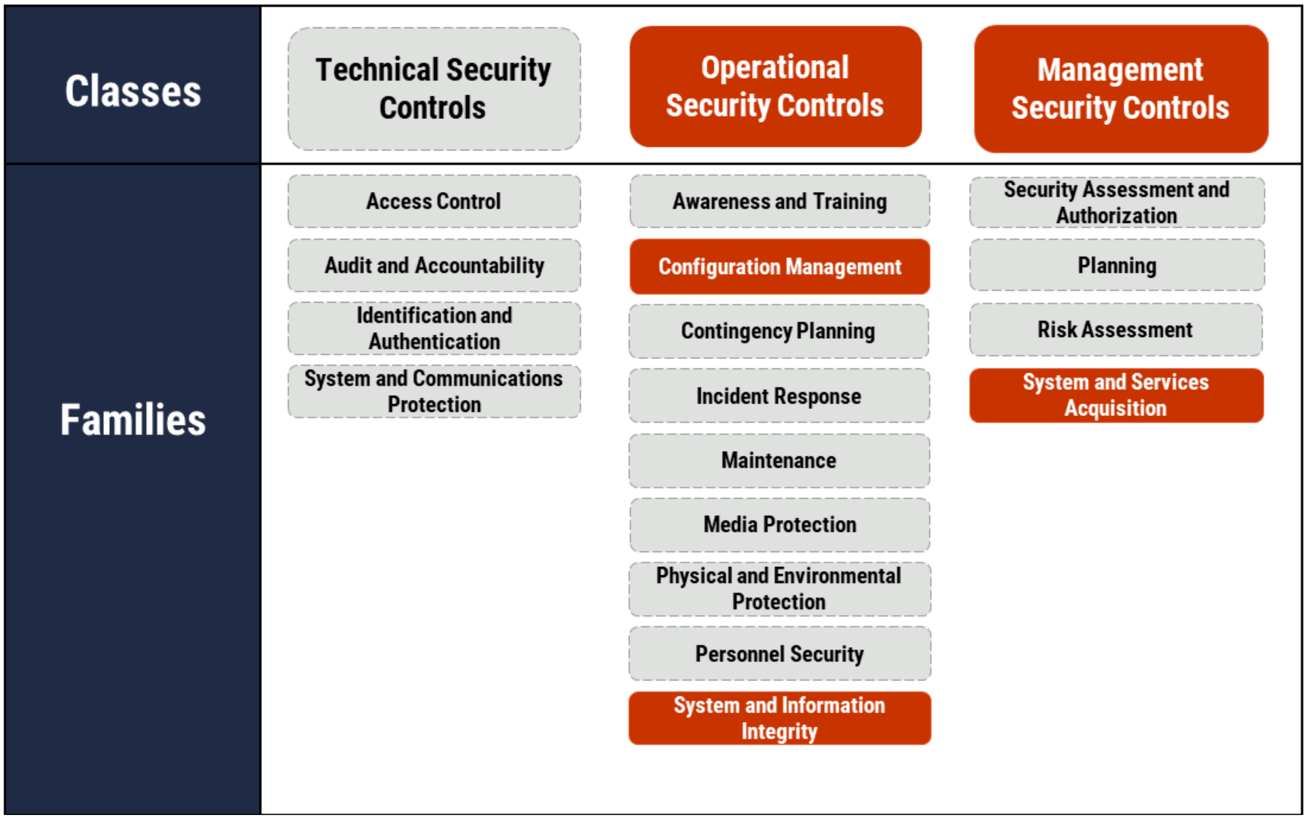
Our top 10 security actions are based on the security controls listed in Annex 3A of ITSG-33 [2]. ITSG-33 [2] is a risk management framework which describes the roles, responsibilities, and activities that help organizations manage their IT security risks and includes a catalogue of security controls (i.e. standardized security requirements to protect the confidentiality, integrity, and availability of IT assets). These security controls are divided into three classes, which are further divided into several families (or groupings) of related security controls:

- **Technical security controls:** Security controls that are implemented and executed by information systems primarily through security mechanisms contained in hardware, software, and firmware components.
- **Operational security controls:** Information system security controls that are primarily implemented and executed by people and typically supported using technology, such as supporting software.
- **Management security controls:** Security controls that focus on management IT security and IT security risks.

As illustrated in Figure 2, the guidance in this document addresses operational security controls that fall under the configuration management (CM) and system and information integrity (SI) families. It also addresses management security controls that fall under the system and services acquisition (SA) family. This document includes actions that satisfy the following security controls:

- **CM-2 Baseline configurations**
- **SI-2 Flaw remediation**
- **SA-22 Unsupported system components**

See Annex A of this document for more information on controls CM-2, SA-22, and SI-2.



Classes	Technical Security Controls	Operational Security Controls	Management Security Controls
Families	Access Control	Awareness and Training	Security Assessment and Authorization
	Audit and Accountability	Configuration Management	Planning
	Identification and Authentication	Contingency Planning	Risk Assessment
	System and Communications Protection	Incident Response	System and Services Acquisition
		Maintenance	
		Media Protection	
		Physical and Environmental Protection	
		Personnel Security	
		System and Information Integrity	

Figure 2: Applicable Security Control Classes and Families Described in ITSG-33

You can use the security controls discussed in this document and in Annex 3A of ITSG-33 [2] as a foundation when determining how to manage your organization's cyber security risks and protect its networks, systems, and IT assets. However, keep in mind that implementing these controls is only one part of the IT security risk management process.

ITSG-33 [2] describes a process based on two levels of risk management activities: departmental-level activities and information system-level activities. These two levels of activities will help your organization identify its security needs for both the entire organization and its information systems. Once you understand your security needs at each level, you can identify which security controls your organization needs to implement and maintain based on your accepted level of risk.

2 Security vulnerabilities and patches

You should always use supported, up-to-date, and tested versions of operating systems and software to ensure that vulnerabilities can be mitigated. When software vendors discover vulnerabilities (i.e. weaknesses or flaws) in their software, they disclose this information and release patches to update the software and address identified vulnerabilities. However, because these vulnerabilities are disclosed publicly, threat actors can use this information to exploit network weaknesses in unpatched systems. To limit your exposure to cyber threats, use your organization's patch management process to assess, test, manage changes, and apply patches as soon as they are released. Note that simply applying a patch without testing it or assessing the impact it may have on your systems and software can cause flaws or issues that may be costly or time-consuming to fix. You should also have an ongoing inventory of your assets to ensure all the systems, servers, or devices that use the same software or hardware are patched when the vendors make their patches available.

If your organization operates in a cloud environment with a CSP or has leveraged the services of an MSP, you should ensure patch management requirements and emergency patching and updating are included in your service agreements.

We highly recommend that you install patches and updates to ensure the ongoing, positive functionality and security of your systems and devices. However, there are some risks to be aware of when applying patches and updates. Some of these risks include the following examples:

- Installing a patch can interfere with the functions in other applications or the functionality of your device (e.g. scheduled time for reboot).
- Rebooting devices for updates might interrupt other programs, resulting in loss of data or disruption of service.
- Installing patches may reveal other issues with the program, including other security flaws (i.e. patching should be approached as a continual process for your organization's IT operations).

2.1 Vulnerability and patch notification

Vendors typically publish the following information about a known vulnerability and the patch to fix that vulnerability:

- Products and versions affected
- Technical details about the vulnerability, including how it may be exploited
- Consequences of an exploitation (e.g. code execution, information spillage or disclosure, denial of service)
- Current exploitation status (i.e. whether the vulnerability is already being exploited)
- Temporary workarounds
- Level of severity of the vulnerability

Vendors communicate the severity of a vulnerability in different ways. For example, the severity may be based on a standard, such as the Common Vulnerability Scoring System (CVSS), or a vendor-defined categorization, such as *critical* or *important*. You should use the severity ratings to do an initial assessment of the likelihood and the impact of the vulnerability being exploited in your organization's environment.

A vendor may also publish a consolidated bulletin that includes recommended deployment instructions for a patch.

2.2 Vulnerability and patch risk assessment

After analyzing the information provided by the vendor, you should assess your organizational risk based on the known vulnerability and the patch. By completing a risk assessment, your organization can determine the level of severity within your specific environment. Even if a threat is common to many different organizations, your organization may be impacted differently.

You should identify all the information systems that are affected by the known vulnerability. When conducting a risk assessment, consider that your risk may increase if an exploit impacts high-value or high-exposure assets. Your risk may decrease if you already have mitigation controls implemented. Your risk may also decrease if the impacted assets have a low risk of exposure.

Table 1 includes examples of the various risk levels based on the vulnerability.

Table 1: Examples of Vulnerability Risk Assessments

Risk Level	Examples
Extreme risk	Vulnerability allows remote code execution Critical business systems and information are affected Exploits exist and are in use System is connected to the Internet and doesn't have mitigation controls in place
High risk	Vulnerability allows remote code execution Critical business system information is affected Exploits exist and are in use System is in a protected enclave with strong access controls
Medium risk	Vulnerability allows attacker to impersonate a legitimate user on a remote access solution System is exposed to unauthenticated users System requires two-factor authentication and administrator-level remote log-in is disallowed
Low risk	Vulnerability requires authenticated users to perform malicious actions (e.g. SQL injection) Affected system contains non-sensitive, publicly available information Existing mitigation controls make exploitation unlikely or very difficult

Table 2 includes a simplified example of patch risk assessments to determine the level of risk if a patch is not applied. In this example, a common vulnerability (critical software remote code execution vulnerability) is being assessed by three organizations that have different security actions implemented in their environments.

Table 2: Example of Patch Risk Assessments Using Critical Software Remote Code Execution Vulnerability

Organization	Security Actions in Place	Patch Risk Assessment
Organization A	None	Extreme
Organization B	Effective email content filtering Low-privileged users	High
Organization C	Effective email content filtering Application allow list Low-privileged users	Medium

3 Baseline configurations for systems (CM-2)

The guidance in this section is based on control **CM-2 Baseline Configuration**. Subsections 3.1-3.4 include ways to enhance your baseline configuration; these enhancements are based on the control enhancements for CM-2. See section A.1 of Annex A for more information.

While updating your systems and software will reduce your organization's exposure to threats, you should develop, document, and maintain a baseline configuration for your systems. Your baseline configuration is the basis for any future builds, releases, and changes to your systems. System updates, removals, and additions could change the behaviour of your system, and a baseline will help you determine and define the cause of potential flaws and problems.

Your baseline configuration should include the following information about the information system components:

- Standard software packages installed on workstations, servers, network components, or mobile devices
- Current version numbers and patch information on operating systems and applications
- Configuration settings and parameters

The baseline should also include information about the network topology, the logical placement of the components within the system architecture, and the security measures implemented. Be sure to compare the configuration of firewalls and routers on each device to make sure no unauthorized changes have been made.

You should store your baseline configuration documents and diagrams in a trusted environment that is separated from the standard operating system.

3.1 Reviews and updates

To maintain your baseline configuration, you need to assess system changes and determine whether a new baseline will need to be created. Baseline maintenance should be integrated with your change management process. Your organization is responsible for defining the frequency and the circumstances for reviewing and updating the baseline, but it should be reviewed and updated when you install and upgrade information system components.

Using an automated mechanism can help your organization maintain an up-to-date, complete, accurate, and readily available baseline configuration. Some examples of automated mechanisms include hardware and software inventory tools, configuration management tools, and network management tools.

3.2 Previous configurations

Your organization should retain previous versions of baseline configurations (e.g. hardware, software, firmware, configuration files, and configuration records). Previous versions will support any system rollbacks that may be required if there are flaws or issues with updates and changes.

3.3 Development and test environments

You should maintain a baseline configuration for any development and test environments. You should manage this baseline separately from your operational baseline.

By having a separate baseline for your development and test environments, you can protect your operational systems from unplanned and unexpected events that may result from development and testing activities. You can also use the separate baselines to manage configurations appropriately. For example, although you need stability to manage operational configurations, greater flexibility is needed when managing configurations in development and test environments.

3.4 Configurations when travelling

If your organization has employees who travel to foreign countries, you should consider how this travel may impact the security of systems and devices. Treat all devices that have been abroad with additional security controls and develop a process that addresses how to assess these devices to decide your next steps. In some cases, you may be able to reintegrate them into organizational networks and systems. However, reintegrating these devices can put your organization at serious risk. You may decide to sanitize and reinitialize the devices, or dispose of them, when employees return from travel.

4 Patch management (SI-2)

The guidance in this section is based on control **SI-2 Flaw Remediation**. See section A.2 of Annex A for more information on this control.

Your organization's business success relies on your ability to maintain trustworthy systems. Your organization should identify, report, and correct information system flaws and vulnerabilities as soon as possible. Patch management is your strategy and process for acquiring, validating, testing, and installing patches and upgrades on your systems and devices. You can use automated patch management software, which can help with receiving, validating, testing, and installing patches.

To maintain the trustworthiness of your systems, your organization should not treat patch management as a low-priority security measure. Your organization protects its networks, systems, and IT assets and strengthens its cyber security posture by staying up to date on patches. Your patch management process should include the following actions:

- Identifying when a new patch has become available for your device
- Testing the patch (when possible) to ensure it is compatible with your existing software and environment
- Reviewing additional requirements that may be necessary for the patch to be installed or function as expected
- Sending notifications when patches are available
- Installing the patches
- Verifying that the patches have been applied successfully

For personal devices, setting up auto-updates is recommended as a form of patch management. Although auto-updating does not test patches, it keeps devices as secure as possible by taking the appropriate measures that are available as soon as possible.

When outsourcing your IT services to a CSP, the Shared Responsibility Model (SRM) is a key factor in determining responsibilities and required actions of your organization and the CSP. The SRM defines where the CSP's responsibilities for security end and where the responsibilities of your organization begin. In general, the CSP is responsible for the security of the cloud and your organization is responsible for the data stored within the cloud. If you have outsourced your IT services to a CSP or an MSP, ensure you include patch management in your SRM. Your service contract should also include your SRM to identify the roles and responsibilities related to patch management, which will vary depending on your cloud service model. For example, in the case of an infrastructure as a service (IaaS) or a platform as a service (PaaS) model, you are responsible for updating and patching your systems and applications. In a software as a service (SaaS) model, the CSP is responsible for updating and patching. However, even if you are using a service provider, you are still responsible for updating and patching any service-related applications, systems, and devices that fall out of the scope of the contract.

4.1 Patch application timeline

Once you have assessed your organization's risk levels and the applicability of the patch within your environment, you should deploy the patch as soon as possible. Your organization should have a policy on patch maintenance. This policy should establish a timeframe for applying corrective actions to vulnerabilities. Timely patch maintenance reduces your organization's exposure to threats.

The timeframe within which you deploy a patch may vary depending on the levels of risk associated with the vulnerability and the patch. We recommend that you use the following timeframes:

- **Extreme risk level**: Within 48 hours
- **High risk level**: Within two weeks
- **Medium risk level**: At next major update or within three months
- **Low risk level**: At next major update or within one year

4.2 Patch testing

Many software vendors thoroughly test patches before releasing them to the public. This testing is usually performed against a range of environments, applications, and conditions. However, your organization is responsible for carrying out additional testing on patches to determine how it will affect your environment.

You should begin by deploying a patch to a test group that includes employees from all business units across the organization (e.g. finance, human resources, operations). If the test group does not report any fault within 48 hours of testing, then the patch can be deployed to the rest of the organization.

4.3 Patch deployment

Before installing a new patch, the system administrators should read all the relevant contextual information about the patch. This information provides details about that patch and what is needed to install it. Additional research may also be useful. For example, external research may show that there are issues when installing a patch.

Automatic updates to software and firmware ensure that patches are installed as soon as possible. However, you should consider your organization’s need to manage and maintain system configurations and the possible impact that automatic updates may have on your business operations.

Mobile operating system patches are generally not performed automatically and require user interaction to apply the patches and update the operating system. Your organization should implement a policy to ensure users apply patches to their mobile devices’ operating system when notified by their mobile carrier. Some mobile vendors may support enterprise-wide automatic operating system updates for mobile devices for an additional service fee.

Be sure to remove previous versions of software and firmware components after updated versions have been installed.

4.4 Workarounds

If a patch is not yet available, but a vulnerability is discovered, vendors may publish temporary fixes or workarounds. For example, these workarounds may include disabling the vulnerable functionality within the software or device or restricting or using firewalls and other access controls to restrict or block access to the vulnerable service. For mobile devices, workarounds may include restricting functionality or implementing a deny list for certain applications, often using mobile device management (MDM) or unified endpoint management (UEM) software.

Like patching, the decision on whether to implement a temporary workaround is a risk-based decision. You should only use temporary workarounds for operating system and software vulnerabilities or problems if a patch is not yet available. We recommend that you track all implemented workarounds to ensure patches are downloaded to overlay and support each other (rather than workarounds overlapping each other). Managing all your implemented workarounds can be challenging if they are not adequately tracked and documented. If a required workaround is removed, your organization risks exposing vulnerable systems and software to threats.

Workarounds are not a permanent solution. Once the patch is available, you should apply it as soon as possible and the workaround should be removed. Your organization should also implement other mitigation controls, such as an intrusion prevention system (IPS) and a web application firewall (WAF), to add layers of defence when a patch is delayed or unavailable.

4.5 Continued monitoring and assessment

Once a patch is installed, system administrators should audit it to measure the success rate and ensure that it is effective and subscribe to your vendor's security alerts and threat intelligence feeds as an additional mitigation measure. Your system administrators should also stay up to date on network, operating system, application vendor, and patch updates so that they can know when new vulnerabilities are discovered and when to apply patches. In addition, monitoring externally for the known vulnerabilities that are meant to be addressed by the patch and ensure there have been no attempted or actual exploitation of your organization's systems.

To address vulnerabilities and flaws in your information systems, you should take advantage of available resources such as the common weakness enumeration (CWE) or common vulnerabilities and exposures (CVE) databases.

4.6 Patch management for critical systems

Patching may require downtime that may have serious operational consequences on critical systems that may be required to operate 24/7, such as industrial control systems (ICS) or operational technology (OT). Due to this requirement, you must develop a cohesive patch management plan that involves personnel from IT, IT security, process engineering, operations, and senior management.

If a system needs continuous operation, you may not be able to remove a device for firmware updates. If this is the case, your organization should assess and approve its risk tolerance and implement other security measures to enhance the security of the system.

5 Unsupported systems and software (SA-22)

This section is based on control **SA-22 Unsupported System Components**. Subsection 4.1 includes guidance on alternative sources for support, which is on the control enhancement for SA-22. See section A.3 of Annex A for more information.

Unsupported devices, operating systems and software are those for which vendors no longer issue updates or patches. Legacy and unsupported devices are susceptible to vulnerabilities that will never be patched, which increases your organization's level of risk. If systems and software cannot be updated, then threat actors can continue to exploit vulnerabilities that may exist.

You should replace system components and software when support (e.g. software patches, firmware updates, maintenance contracts) from the developer, vendor, or manufacturer is no longer available. However, there may be exceptions that prevent your organization from replacing unsupported system components and software. For example, you may be using unsupported systems that provide critical business capability, but newer technologies are not available to replace them.

It is important that your organization has an IT systems lifecycle in place. By using a lifecycle, your organization can effectively manage the disposal of its old, unsupported systems and software and the implementation of modern software. Using unsupported software can introduce serious risks to your organization and is not recommended. If your organization accepts the risk of using unsupported systems and software, you should document the justification and approval for their continued use.

5.1 Alternative sources for support

If support is no longer provided by the original developer, vendor, or manufacturer, your organization may choose to set up in-house support. For example, your organization may develop customized patches for critical software components or set up contracted services with external providers (e.g. open source software vendors) who can provide ongoing support for unsupported systems and software.

A risk assessment for continuing to use unsupported software with respect to the potential for security vulnerabilities should be completed. Ultimately, your organization should begin a process to abandon unsupported software and systems and migrate to supported products.

You should also consider mobile devices that are used by your organization that may have personally-installed applications. While you are not responsible to support these apps, as they are not designated for business purposes, the presence of them on business mobile devices may increase the risk to your organization. If you have permitted personally-installed applications (e.g. you have a bring-your-own-device (BYOD) model) the user should be made responsible for tracking vulnerabilities and updating these applications as updates are made available. If the risks associated with personally-installed applications is too great for your organization, consider a different deployment model or implement controls such as policies and procedures, to ensure users maintain pathing on these personal applications and remove them when they are no longer supported by the developer.

6 Summary

One of our top 10 recommended IT security actions is to apply patches for operating systems and applications. This document outlines our recommended best practices for patching. These best practices are based on security controls CM-2, SI-2, and SA-22, which are detailed in Annex A of this document. Applying patches reduces your organization's exposure to threats that could exploit publicly known vulnerabilities and compromise your networks, systems, and IT assets.

However, patching is just one aspect of improving your cyber security posture. To best protect your organization against cyber threats, you should review and implement all the actions recommended in ITSM.10.089 [1].

6.1 Contact information

For more information on implementing this guidance or any of the other top 10 security actions, email, or phone our Contact Centre:

Contact Centre
contact@cyber.gc.ca
(613) 949-7048 or 1-833-CYBER-88

7 Supporting content

7.1 List of abbreviations

Term	Definition
CM	Configuration management (security control family code)
CVE	Common vulnerabilities and exposures
CVSS	Common vulnerability scoring system
CWE	Common weakness enumeration
IT	Information Technology
SA	System and services acquisition (security control family code)
SI	System and information integrity (security control family code)

7.2 Glossary

Term	Definition
Availability	A value that is assigned to information assets, software, and hardware (infrastructure and its components). Data with the highest possible availability rating must always be accessible. Implied in its definition is that availability includes the protection of assets from unauthorized access and compromise.
Confidentiality	A value that is assigned to a set of information to indicate its sensitivity level and any access restrictions that prevent unauthorized people from accessing it.
Cyber attack	The use of electronic means to interrupt, manipulate, destroy, or gain unauthorized access to a computer system, network, or device.
Integrity	A value that is assigned to information to indicate how sensitive it is to data loss. Implied in its definition is that integrity includes protecting information from being modified or deleted unintentionally or when it's not supposed to be. Integrity helps determine that information is what it claims to be. Integrity also applies to business processes, software application logic, hardware, and personnel.
IT asset	The components of an information system, including business applications, data, hardware, and software.
Management security control	A class of security controls that focus on the management of IT security and IT security risks.
Operational security control	A class of security controls primarily implemented and executed by people and typically supported by technology (e.g. supporting software).
Risk	The likelihood and the impact of a threat using a vulnerability to access or compromise IT assets.
Security control	A management, operational, or technical high-level security requirement needed for an information system to protect the confidentiality, integrity, and availability of its IT assets. Security controls can be applied by using a variety of security solutions, including security products, security policies, security practices, and security procedures.

Term	Definition
Technical security control	A class of security controls that are implemented and executed by information systems primarily through security mechanisms contained in hardware, software, and firmware components.
Threat	Any potential event of act (deliberate or accidental) or natural hazard that could compromise IT assets and information.
Vulnerability	A flaw or weakness in the design or implementation of an information system or its environment that could be exploited by a threat actor to adversely affect an organization's assets or operations.

7.3 References

Number	Reference
1	Canadian Centre for Cyber Security. *ITSM.10.089 Top 10 Information Technology Security Actions to Protect Internet-Connected Networks and Information*. October 2021.
2	Canadian Centre for Cyber Security. *ITSG-33 IT Security Risk Management: A Lifecycle Approach*. December 2014.
3	Canadian Centre for Cyber Security. *ITSM.50.062 Cloud Security Risk Management*. March 2019.
4	Canadian Centre for Cyber Security. *ITSM.50.030 Cyber Security Considerations for Consumers of Managed Services*. October 2020.

Annex A ITSG-33 security control catalogue

A.1 Operational security controls: configuration management

Table 3 lists the configuration management (CM) controls, as defined in Annex 3A of ITSG-33 [2].

Table 3: ITSG-33 Operational Security Controls: Configuration Management (CM)

Number	Control	Requirement	Control Enhancements	Related ITSG-33 Controls
CM-2	Baseline configuration	(A) The organization develops and documents a current baseline configuration of the information system. This baseline configuration is maintained under configuration control.	**Reviews and updates:** The organization reviews and updates the baseline configuration of the information system: i. [*Organization-defined frequency*] ii. When required due to [*organization-defined circumstances*] iii. As an integral part of information system component installations and upgrades See related control CM-5.	CM-3 CM-6 CM-8 CM-9 SA-10
			Automation support for accuracy and currency: The organization uses automated mechanisms to maintain an up-to-date, complete, accurate, and readily available baseline configuration of the information system. See related controls CM-7 and RA-5.	
			Retention of previous configurations: The organization retains [*organization-defined previous versions of baseline configurations*] to support rollback.	
			Development and test environments: The organization maintains a baseline configuration for information system development and test environments that is managed separately from the operational baseline configuration. See related controls CM-4, SC-3, and SC-7.	

			Configure systems, components, or devices for high-risk areas: i. The organization issues [*organization-defined information systems, system components, or devices*] with [*organization-defined configurations*] to individuals travelling to locations that the organization deems to be of significant risk. ii. The organization applies [*organization-defined security safeguards*] to the devices when the individuals return.	

A.2 Management security controls: system and information integrity

Table 4 lists the system and information integrity controls as defined in Annex 3A of ITSG-33 [2].

Table 4: ITSG-33 Management Security Controls: System and Information Integrity

Number	Control	Requirement	Control Enhancements	Related ITSG-33 Controls
SI-2	Flaw remediation	(A) The organization identifies, reports, and corrects information system flaws. (B) The organization tests software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation. (C) The organization installs security-relevant software and firmware updates within [*organization-defined time period*] of the release of the updates. (D) The organization incorporates flaw remediation into the organizational configuration management process.	**Central management:** The organization centrally manages the flaw remediation process. **Automated flaw remediation status:** The organization uses automated mechanisms [*organization-defined frequency*] to determine the state of information system components regarding flaw remediation. This control enhancement has the following related controls: CM-6 and SI-4. **Time to remediate flaws and benchmarks for corrective actions:** The organization: i. Measures the time between flaw identification and flaw remediation ii. Establishes [*organization-defined benchmarks*] for taking corrective actions **Automatic software and firmware updates:** The organization installs [*organization-defined information system components*]. **Removal of previous versions of software and firmware:** The organization removes [*organization-defined software and firmware components]* after updated versions have been installed.	CA-2 CA-7 CM-3 CM-5 CM-8 MA-2 IR-4 RA-5 SA-10 SA-11 SI-11

A.3 Operational security controls: system and services acquisition

Table 5 lists the system and services acquisition (SA) controls as defined in Annex 3A of ITSG-33 [2].

Table 5: ITSG-33 Operational Security Controls: System and Services Acquisition

Number	Control	Requirement	Control Enhancements	Related ITSG-33 Controls
SA-22	Unsupported system components	(A) The organization replaces information system components when support for the components is no longer available from the developer, vendor, or manufacturer. (B) The organization provides justification and documents approval for the continued use of unsupported system components required to satisfy mission/business needs.	**Alternative sources for continued support:** The organization provides [*selection (one or more): in-house support;* [*Assignment: organization-defined support from external providers*]] for unsupported information system components.	PL-2 SA-3