Communications Security Establishment
Centre de la sécurité des télécommunications

CANADIAN CENTRE FOR
CYBER SECURITY

Top 10 IT security actions:

No. 7 protect information at the enterprise level

MANAGEMENT

ITSM.10.097

Canada

Foreword

This document is an UNCLASSIFIED publication that is part of a suite of documents that focus on each of the top 10 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 February 9, 2022.

Revision history

Revision	Amendments	Date
1	First release.	February 9, 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 manage information at the enterprise level. Your organization's information is not only valuable to your continued operation, but also a valuable target to threat actors who are looking to compromise your systems and information.

To protect your organization's information at the enterprise level, some of the actions you should take include the following: assess and identify its value, manage it throughout its lifecycle, choose the right enterprise mobility model, use external information systems securely, and set up a compliance monitoring program.

This document is part of a suite of documents that focus on each of 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 cyber security actions, email or phone our Contact Centre:

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

D97-4/10-097-2023E-PDF

978-0-660-46921-8

Table of contents

1 Introduction 6

1.1 Top 10 IT security actions 7

1.2 IT security risk management 8

2 Threats to your enterprise information 10

2.1 Common threats 10

2.2 Insider threats 12

2.3 Threats to your supply chain 12

3 Assess your enterprise information 13

3.1 Identify its value (RA-2) 13

3.2 Classify and categorize (RA-2) 13

4 Manage your information 14

4.1 Retention and disposition (SI-12 and MP-6) 14

4.2 Inventories and tracking (CM-8) 15

4.3 Backups (CP-9) 15

5 Manage your mobile devices 16

5.1 Enterprise mobility models (MP-7 and SA-9) 16

5.1.1 COBO model 17

5.1.2 COPE model 17

5.1.3 CYOD model 17

5.1.4 BYOD model 17

5.2 Travel and mobile devices 18

6 Secure external information systems 19

6.1 Identify the associated risks (AC-20 and SA-9) 19

6.2 Document agreements (AC-20 and SA-9) 20

7 Set up compliance monitoring 21

7.1 Continuous monitoring (AU-1) 21

8 Summary 22

8.1 Contact information 22

9 Supporting Content 23

9.1 List of Abbreviations 23

9.2 Glossary 23
9.3 References 24

List of figures

Figure 1: Top 10 IT security actions – no. 7 protect information at the enterprise level 7
Figure 2: Applicable security control classes and families described in ITSG-33 9

List of tables

Table 1: Examples of common threats to enterprise information 10
Table 2: ITSG-33 technical security controls: access control 26
Table 3: ITSG-33 technical security controls: audit and accountability 28
Table 4: ITSG-33 operational security controls: configuration management 29
Table 5: ITSG-33 operational security controls: contingency planning 31
Table 6: ITSG-33 operational security controls: media protection 33
Table 7: ITSG-33 operational security controls: system and information integrity 35
Table 8: ITSG-33 management controls: risk assessment 36
Table 9: ITSG-33 management security controls: system and services acquisition 37

List of annexes

Annex A ITSG-33 security control catalogue 26
A.1 Technical security controls: access control 26
A.1.1 Access control 26
A.1.2 Audit and accountability 28
A.2 Operational security controls 29
A.2.1 Configuration management 29
A.2.2 Contingency planning 31
A.2.3 Media protection 33
A.2.4 System and information integrity 35
A.3 Management security controls 36
A.3.1 Risk assessment 36
A.3.2 System and services acquisition 37

1 Introduction

This document provides guidance on the measures that your organization can take to protect information at the enterprise level. This guidance is based on the advice that we provide in ITSM.10.089 [1] and the security controls listed in Annex 3A of ITSG-33 IT Security Risk Management: A Lifecycle Approach [2].

To protect your organization's information at the enterprise level, you need to take steps to manage risk, comply with legislative and policy requirements, and implement security controls. This document outlines some of the measures you can take. These actions include the following examples:

- assessing and identifying the value and sensitivity of information
- managing information throughout its lifecycle (e.g. data labelling, handling, retention, and destruction)
- choosing an enterprise mobility model to help you manage devices used in your organization
- understanding the risks associated with using external information systems
- setting up a compliance monitoring program

The guidance in this document is not comprehensive or all-encompassing. It only outlines some of the security controls that you can implement to protect your organization's information. Refer to Baseline Cyber Security Controls for Small and Medium Organizations [3] for more information on the security controls that you can implement to protect your organization at a general and minimum level.

Before implementing any security measures, you should conduct a risk assessment to help you identify your organization's specific security requirements. Once you understand your specific risk profile, you can scope and tailor this advice to align with your organization. You should take steps to identify and determine the controls that your organization needs to protect its assets; implementing unnecessary controls can lead to inefficiencies and unnecessary expenses. Once you have identified the controls that best suit your organization's needs, you should tailor them so that they meet your organization's specific environment and requirements.

1.1 Top 10 IT security actions

Our top 10 recommended IT security actions, which are listed in Figure 1, are based on our analysis of trends in cyber security threat activities and the impact of those threat activities on Internet-connected networks.
By implementing all 10 of these actions, you can address many of your organization's IT security vulnerabilities. However, your organization is unique. To ensure your organization's security needs are appropriately met, review your current security and risk management activities.

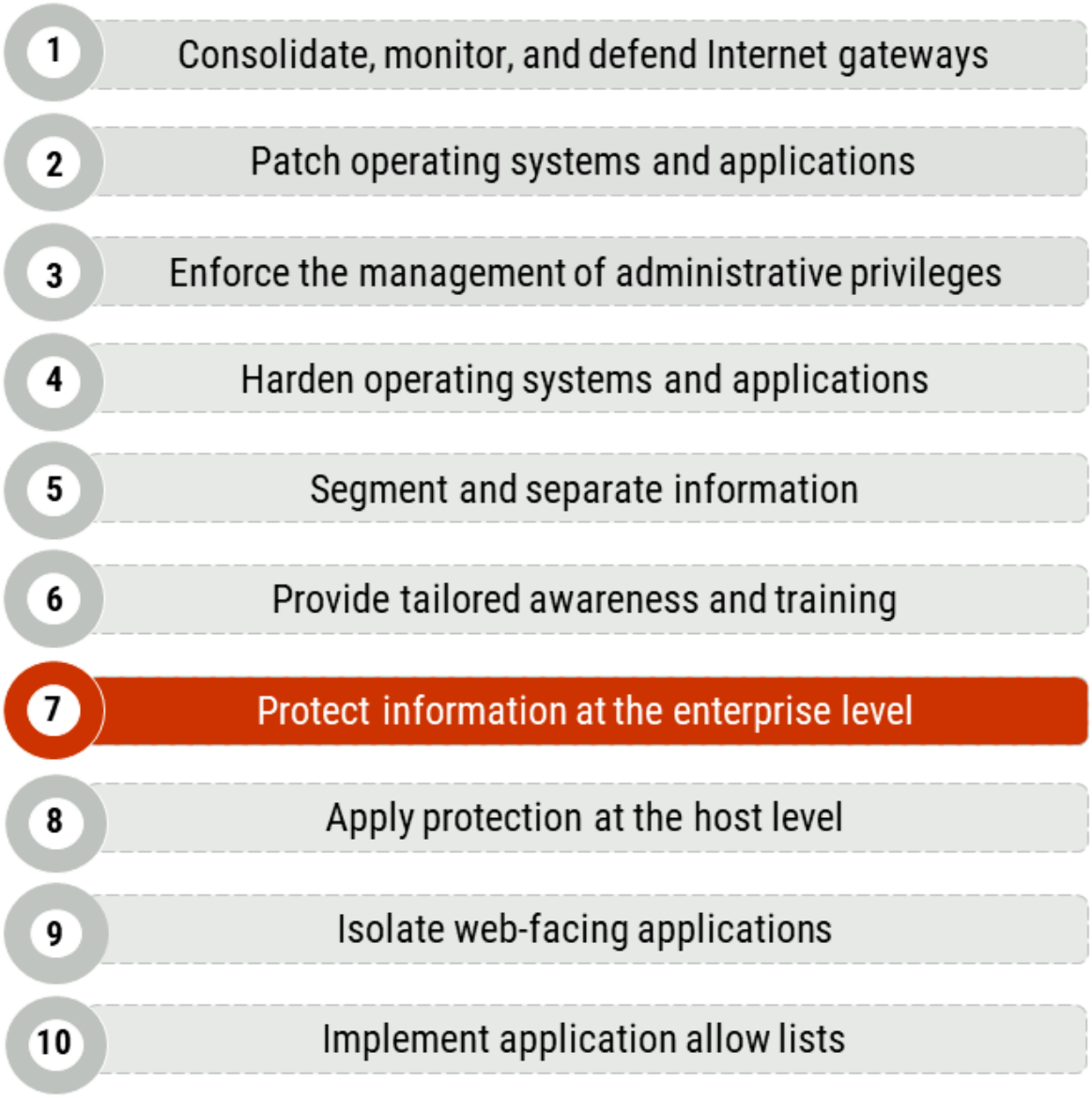

Figure 1: Top 10 IT security actions – no. 7 protect information at the enterprise level

1.2 IT security risk management

Our top 10 security actions are taken from the security controls listed in Annex 3A of ITSG-33 [2].
ITSG-33 [2] 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 is based on several different technical, operational, and management security controls, including the following examples:

- **Access Control (AC)**: AC-20 Use of External Information Systems
- **Audit and Accountability (AU)**: AU-1 Audit and Accountability Policies and Procedures
- **Configuration Management (CM)**: CM-8 Information System Component Inventory
- **Contingency Planning (CP)**: CP-9 Information System Backup
- **Media Protection (MP)**: MP-6 Media Sanitization and MP-7 Media Use
- **Risk Assessment (RA)**: RA-2 Security Categorization
- **System and Information Integrity (SI)**: SI-12 Information Output Handling and Retention
- **System and Service Acquisition (SA):** SA-9 External Information System Services

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 for managing your organization's cyber security risks. However, implementing controls is only one part of the IT security risk management process.

ITSG-33 [2] also describes an IT security risk management process that is 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 the accepted level of risk.

2 Threats to your enterprise information

Your organization needs to constantly adapt to changing technologies so that it can protect its networks, systems, IT assets, sensitive data, and information from emerging cyber threats. The increase in mobile and Internet-connected devices and the rising demand for remote and flexible working arrangements bring new challenges associated with protecting enterprise information.

Your organization may also rely on systems and services that are provided by other organizations. For example, your organization may use cloud services or third-party applications to store business information. The less control you have over the systems and devices that process, store, or transmit business information, the less confident you can be that the information is secure. Regardless of changing technologies and challenges, your organization is always responsible for protecting the confidentiality, integrity, and availability of your networks, systems, and information.

2.1 Common threats

If a threat actor successfully exploits and compromises your organization's network, systems, and information, your organization may be at serious risk. You may not be able to carry out business activities, your organization's data may be stolen or leaked, and you may experience financial loss. Data breaches can damage your organization's reputation, jeopardize your business relationships, and impact the privacy of your employees, partners, and customers. Table 1 outlines some examples of common threats to enterprise information.

Table 1: Examples of common threats to enterprise information

Threat	Description	Impact
Malware	Malicious software designed to infiltrate or damage a computer system. Common forms of malware include computer viruses, worms, Trojans, spyware, and adware. For example, ransomware is a type of malware that denies a user's access to a system or data until a sum of money is paid.	Once malware is on your systems, a threat actor can use it to create an entry point into your systems, steal information, or damage systems. In a ransomware attack, a threat actor encrypts organizational data and compromises data availability. Threat actors demand payment before decrypting the information; however, even if you pay, they may not decrypt the information.
Viruses	A computer program that spreads by making copies of itself. Computer viruses spread from one computer to another, usually without the knowledge of the user.	Viruses can have harmful effects, ranging from displaying irritating messages to stealing data or giving other users control over the infected computer.
Phishing	An attempt to get confidential information (e.g. personal information, credit card numbers) from an individual, group, or organization by mimicking or spoofing, a specific, usually well-known brand.	A threat actor gains access to user credentials and sensitive data (e.g. intellectual property, financial information, personal information). A threat actor can sell this information or use it to commit fraud.

Threat	Description	Impact
Backdoor	A backdoor is a point of entry into a system or computer, bypassing authentication measures, encryption, or intrusion detection systems. Backdoors are often created deliberately for troubleshooting, software updates, or system maintenance. Threat actors can use these legitimate backdoors for malicious purposes.	Once threat actors have this remote access, they can steal information, install malware, or control the device's processes and procedures.
Denial-of-service (DoS) attack Distributed denial-of-service (DDoS) attack	A DoS attack attempts to disrupt the normal activities of a specific host (e.g. website, server, network) by overwhelming it with Internet traffic (requests). The overall objective is to make the host unavailable for legitimate requests from users and render the targeted system dysfunctional. A DDoS attack introduces traffic flooding from multiple sources (e.g. from a botnet). A DDoS attack is more difficult to stop. It's also difficult to distinguish legitimate user traffic from malicious traffic.	The host is unavailable for legitimate requests from users and render the targeted system dysfunctional. For example, your organization's website becomes unavailable until you stop the attack.
Person-in-the-middle (PITM)	An attempt to intercept communications between two parties (e.g. a user and a web server) without the user's knowledge. The user believes they are communicating directly and securely with a website. PITM attacks can be achieved through different techniques (e.g. phishing, Wi-Fi eavesdropping).	PITM attacks enable threat actors to monitor communications, reroute traffic, alter information, deliver malware, and acquire personal or other sensitive information.
Password cracking	An attempt to access accounts directly. Two common forms of password cracking are brute-force and dictionary-based attacks. In a brute-force attack, a threat actor uses an exhaustive number of randomly generated passwords to guess the correct one. In dictionary-based attacks, a threat actor uses a list of commonly used passwords to try guessing the correct password.	If a threat actor successfully cracks a password to an account, they gain access to sensitive information. A threat actor can potentially access to other accounts if the victim has used the same password for several accounts.
Natural disasters and fires	Natural disasters, such as earthquakes and floods, and fires can also cause harm to your organization's systems and information.	The availability of your organization's information and services is jeopardized if systems and information are damaged or destroyed. If you don't have backups that are stored in a different location, then your organization may experience financial loss or legal risk.

2.2 Insider threats

An insider threat is any individual who has knowledge of or access to your organization's infrastructure and information and who uses, either knowingly or inadvertently, the infrastructure or information to cause harm. Insider threats can put your organization's employees, customers, assets, reputation and interests at risk.

Generally, when we think of an insider threat, we think of someone who knowingly wants to cause harm. An individual may carry out targeted attack by abusing privileged access or general accounts to install malware or steal sensitive information.

However, anyone who has access to your organization's infrastructure or information (e.g. employees, contractors, or service providers) can cause harm inadvertently. For example, inadvertent insider threats can be caused by the following behaviours:

- misplacing a mobile device or removable media
- granting user access to sensitive information beyond what is required for a person's job functions
- mishandling sensitive information (e.g. storing it improperly, not applying protective markings or distribution caveats)

An insider threat can affect the confidentiality, integrity, and availability of your organization's systems and information. For example, an insider threat may unintentionally disclose sensitive information or intentionally steal intellectual property, disrupt organizational services, or destroy critical information.

For more information, see ITSAP.10.003 How to Protect Your Organization from Insider Threats [4].

2.3 Threats to your supply chain

You should ensure that you manage the risks associated with your supply chain as part of your cyber security plan and risk management activities. Your supply chain includes any of the suppliers, services, equipment, software, or processes your organization uses.

Even with a robust cyber security program in place, your organization's systems and information are at risk if your supply chain is compromised. Threat actors may try to compromise the supply chain by infiltrating trusted suppliers and vendors, violating the assumed trust that you might have with suppliers and vendors.

For more information on protecting your supply chain, see ITSAP.00.070 Supply Chain Security for Small and Medium Organizations [5].

3 Assess your enterprise information

The guidance in this section is based on security control **RA-2 Security Categorization**.

Without a complete understanding of the information that your organization processes and holds, you cannot fully protect it. As a part of your risk management and cyber security activities, you should examine your enterprise information to identity its value, classify it based on its level of sensitivity, and categorize it in groups.

3.1 Identify its value (RA-2)

By identifying the value of your organization's information, you can prioritize what needs to be protected.

You can determine the value of your organization's information by assessing the possible harm that could result from the inability to protect its confidentiality, integrity, and availability. When assigning value, consider the following types of information:

- **Business critical information:** Information that your organization relies on for its ongoing operation (e.g. sales information, emergency response plans).
- **Sensitive information:** Information that needs to be kept confidential or only accessed by certain people (e.g. financial or personal information, intellectual property).
- **Records and evidence**: Information that needs to be protected from unauthorized modification (e.g. contracts, receipts).

For more information on determining the value of information systems and assets, see ITSAP.40.001 Protecting High-Value Information: Tips for Small and Medium Organizations [6] and section 2.3 of our Baseline Cyber Security Controls for Small and Medium Organizations [3].

3.2 Classify and categorize (RA-2)

As you identify the value of your enterprise information, you should also classify and organize it into groups or classes based on its level of sensitivity. The classification markings that your organization applies may vary, depending on whether you are a government department or a non-government, private organization. Classifying your information appropriately helps you manage your information and protect your information against unauthorized access and distribution, as well as improper retention and disposition.

Categorizing your enterprise information have several purposes, including the following examples:

- reflects the value that your organization has assigned to the information
- represents your organization's risk tolerance
- determines how your organization assures the confidentiality, integrity, and availability of information

When enterprise information is classified and categorized appropriately, your organization is in a better position to manage it throughout its lifecycle, ensure that it is properly retained and destroyed, and protect it against unauthorized access and distribution. In addition, by understanding your information, you can implement the appropriate security controls and manage risks according to your organization's agreed-upon risk tolerance.

4 Manage your information

The guidance in this section is based on the following security controls: **SI-12 Information Output Handling and Retention**, **MP-6 Media Sanitization**, **CM-8 Information System Component Inventory**, and **CP-9 Information System Backup**. These security controls are just some examples of actions that your organization can implement to manage its information.

To protect your organization's information, you need to ensure that it is properly managed throughout its lifecycle. From the time in which information is created or received, it should be handled according to your organization's policies and to its level of sensitivity.

Providing awareness on the proper handling of information is a critical step in protecting organizational information. Anyone who has access to your organization's infrastructure or information (e.g. employees, contractors, or service providers) can cause harm inadvertently. For example, inadvertent data breaches or leaks can be caused by the following behaviours:

- misplacing a mobile device or removable media
- granting user access to sensitive information beyond what is required for a person's job functions
- storing information improperly (e.g. sensitive information is not encrypted)
- applying incorrect markings or distribution caveats on information (or not applying them at all)

4.1 Retention and disposition (SI-12 and MP-6)

You should ensure that information, records, and media are retained for as long as required for business purposes and legal and regulatory requirements. Information has different retention requirements based on its function. For example, from a legislative and regulatory perspective, you must retain financial information for a longer period than you would for administrative information, such as committee or meeting notes. Your organization is responsible for creating and maintaining a retention schedule that outlines how long information must be kept and its final disposition actions (e.g. destroy, preserve).

When information reaches the end of its lifecycle, you should ensure that it is disposed of properly (e.g. shredding, incinerating, degaussing) to prevent data remanence and breaches. If information or media are not properly destroyed, residual data may remain, or data may be recovered and reconstructed.

Note: If you are reusing physical or electronic media or releasing it out of your organization's control, you must ensure that it is properly sanitized. In some cases, you may want to sanitize media, such as a hard drive, before it is destroyed as an additional layer of security.

If your organization uses cloud service providers (CSPs), you should be aware of some additional challenges to properly destroying information. You have less control over ensuring that information is properly removed from physical assets. You should ensure that you address retention and disposition in your service-level agreement with a service provider. One aspect of data disposal to consider for cloud environments is crypto-shredding. With this method of data disposition, the encryption key assigned to protect the data is purposefully deleted or overwritten. This method can only be applied to data that has been encrypted. Your organization should encrypt sensitive and proprietary data when it is at rest, in transit, and in use in order to ensure you maintain the confidentiality, integrity, and availability of your data.

4.2 Inventories and tracking (CM-8)

Your organization should have an inventory of all your organization's information systems and their components (i.e. hardware, software, databases, networks, people). You are responsible for determining the criteria for the types of information system components (e.g. microprocessors, motherboards, software, programmable logic controllers, network devices) that are included in the inventory.

The information you include about the components should be detailed enough for your organization's tracking and reporting requirements. For each component, you should list its configuration information, including any approved deviations, and the individuals, and their contact information, who are responsible and accountable for the component. Be sure to include system-specific information (e.g. system association, system owner, software license, software versions) and hardware inventory specifications (e.g. manufacturer, device type, model, serial number, and physical location). For networked components or devices, you should also include machine names and network addresses.

Be sure to review this inventory. You should update the inventory in scenarios such as when information systems are updated and when components are installed and removed. You may want to use automated mechanisms so that you can maintain an up-to-date, complete, and accurate inventory.

As part of your inventory maintenance, ensure you review the cryptographic configurations within your software and hardware. To allow for cryptographic agility, your inventory should list the cryptographic algorithms configured for each component. Cryptographic agility is a concept of best practice that enables cryptographic algorithms used in applications and protocols to be interchanged easily to ensure systems remain secure if new cryptographic vulnerabilities are discovered. This is done primarily through configuration without requiring major software or hardware updates. For more information, see ITSAP.40.018 Guidance on Becoming Cryptographically Agile [7].

4.3 Backups (CP-9)

Backing up your organization's information is another step that you can take to protect information. When you back up your information, you are creating a duplicate copy that is stored in a different location. Your organization should determine an appropriate storage location based on your risk assessment and the level of sensitivity of the information.

Backups protect the availability of information if a system is down or compromised. For example, if your organization is the victim of a ransomware attack, you have a separate copy of the information that has been encrypted by a threat actor. If data is lost, you can use the backups to recover the data and continue with business activities.

5 Manage your mobile devices

This section is based on security controls **MP-7 Media Use** and **SA-9 External Information System Services**. This section describes some of the actions that your organization can take to manage its mobile devices; however, your organization should determine whether additional controls are required.

Mobile devices play a critical role in daily business activities, but they can increase the level of risk to your organization and its information. Mobile devices can contain a lot of sensitive and personal information, making them attractive targets to threat actors who are intent on gathering information.

By taking advantage of a compromised device, threat actors can access your organization's networks, systems, and information. Threat actors use different methods to try and gather information, including some of the following examples:

- remotely accessing and controlling devices
- physically tampering with devices
- using location tracking functions on devices
- sending emails and text messages that contain malicious links and attachments

For more information on using mobile devices securely, refer to ITSAP.00.001 Using Your Mobile Device Securely [8] and ITSM.80.001 Securing the Enterprise for Mobility [9].

5.1 Enterprise mobility models (MP-7 and SA-9)

Mobile devices are essential to most organizations, but your organization needs to decide on the ownership model for these devices.

There are four different enterprise mobility models that your organization should consider. Choose a model that best suits your business objectives, security requirements, and risk management framework. The four models include the following:

- Corporately Owned for Business Only (COBO)
- Corporately Owned and Personally Enabled (COPE)
- Choose Your Own Device (CYOD)
- Bring Your Own Device (BYOD)

You should clearly define the mobility model that your organization has in place, ensuring that it aligns with your policy requirements and that employees understand the implications of the model. When choosing a model, ensure that you consider the following aspects:

- Which type of devices are included in this model (e.g. provider, smartphones, tablets, laptops, and other IoT devices)?
- Who is responsible for paying for the device?
- Who manages the devices and who is responsible for supporting it?
- Which applications are authorized to run on the devices?
- How tightly is the device integrated into the enterprise network?

Although there are benefits to integrating mobile devices in the workplace, you need to balance this integration with the ability to reduce risks associated with having unmanaged devices connect to your network.

When deploying mobile devices in your organization, you should consider the risks and benefits of various deployment models. If it makes business sense, your organization should provide equipment (e.g. servers, desktops, laptops, mobile devices) to employees, using a device management framework and a configuration change management process. If your organization chooses to allow employees to use their personal devices for business, you should implement a strict control policy and review technologies and legal requirements for segregating business and personal information. Your organization can use unified endpoint management (UEM) to maintain the security of mobile devices. UEM combines features from mobile device management and enterprise mobility management processes.

5.1.1 COBO model

In a COBO model, mobile devices are supplied and owned by your organization. This model prohibits the use of personal devices for work purposes and the personal use of work devices. If it makes sense in your environment, we recommend that you provide employees with the equipment they require for their work (e.g. servers, desktops, laptops, mobile devices) because it provides your organization with more control over the security controls that are implemented on devices. You can also install antivirus software and other protective measures to secure the devices.

5.1.2 COPE model

In a COPE model, your organization provides employees with devices, but you also allow employees to use these devices as personal devices. With COPE equipment and devices, you have more control over the security controls that are implemented. Additionally, when an employee leaves your organization, you keep the equipment and devices.

You should ensure that sensitive information and your corporate IT infrastructure are secured appropriately. We recommend that you ensure that work and personal data, including applications, email accounts, and contacts, are separated on these devices. There are different solutions available that you can use to separate personal and work data. Some examples of solutions include using separate apps for work or using a secure folder or locker functions for sensitive business information. You should ensure that all sensitive data is encrypted and securely stored.

Your organization needs to take additional measures to protect mobile devices, as they are at a higher risk of being exploited by threat actors than organization-owned devices (e.g. desktops and laptops) that are only used within the workplace and on your organization's networks.

5.1.3 CYOD model

In a CYOD model, you allow your employees to choose from a list of devices that your organization has approved for business use. Your organization selects the devices and continues to manage them, which means that you have more control over the security controls implemented, the applications that run on the devices, and the functions that are available to users.

5.1.4 BYOD model

There are many reasons why your organization may want to allow employees to use their personal devices for work. With a BYOD model in place, your organization benefits by saving money that would otherwise be spent buying mobile devices for all employees and using up-to-date technology that employees are comfortable with.

However, your organization needs to consider the associated security risks before you tell employees that they can use their personal devices. While this section does not cover all the associated risks, you should consider the following:

- How will you manage and support different devices?
- How will you limit the information that is accessed or shared via personal devices?
- What technical controls (e.g. container applications, mobile device management) will you implement?
- What are your legal responsibilities for protecting personal information?
- How will you address security incidents if a personal phone is lost or stolen?
- How will you ensure that information on personal devices is backed up or wiped when an employee leaves the organization?

Conduct a threat and risk assessment (TRA) before you implement a BYOD model. Because the use of personal devices may have privacy impacts, you should assess the privacy risks that may be introduced.

You should also create a policy that informs users of the acceptable use of personal devices and their expected behaviours. Policies should be communicated to your staff through training programs so that you can ensure everyone understands their roles and responsibilities.

For more information on BYOD, refer to ITSM.70.003 End user device security for Bring-Your-Own-Device (BYOD) deployment models [10].

5.2 Travel and mobile devices

There are risks you need to consider if your employees are travelling with work devices. Individuals who hold senior or executive positions are at a higher risk of being targeted by threat actors. Keep in mind that, in some countries, hotel business centres and phone networks may be monitored, and rooms may be searched. When travelling, users should assume that there is no privacy in offices, hotels, Internet cafes, or other public areas.

When determining which locations are of concern, defining required configurations for the devices, ensuring that the devices are configured as intended before travel is initiated, and applying specific safeguards to the device after travel is completed.

Before travelling, you should determine whether the destination or the nature of the event is an area of concern and ensure devices are configured appropriately. You should advise employees to take precautionary measures by disabling features such as Bluetooth and wireless headset capabilities and backing up data on the devices that they are taking with them. Employees should be cautioned not to use unknown, unsecured, or public Wi-Fi networks.

When employees return from a work trip, your IT department should assess all devices before they are connected to organizational systems and networks. You should apply specific safeguards to devices once travel is complete. For example, specific safeguards applied to mobile devices upon return from travel include, examining the device for signs of physical tampering and purging or reimaging the hard disk drive. There may be some scenarios in which it may be appropriate to use dedicated travel or “burner” devices, or even to dispose of the device rather than allowing it back on your network.

6 Secure external information systems

The guidance in this section is based on control **AC-20 Use of External Information Systems** and **SA-9 External Information System Services**. See Annex A.1 of this document for more information on these controls.
This section includes some of the actions you can take to protect your organization from cyber threats and compromises when using external information systems.

Your organization may rely on systems and services that are provided by other organizations. For example, your organization may use cloud services to store business information, or your employees might use their personal devices for work purposes. In this document, we refer to these systems provided by other organizations as *external information systems*.

Your organization may have situations in which employees or other authorized individuals (e.g. contractors) need to access organizational systems through external systems. External information systems may include personally owned devices (e.g. tablets and other mobile devices), privately owned systems and devices that are in commercial or public facilities (e.g. hotels, convention centres, airports), or systems owned or controlled by other organizations (e.g. cloud services). We recommend that you prohibit the use of network-accessible storage devices on external information systems.

6.1 Identify the associated risks (AC-20 and SA-9)

External information systems, such as Internet and Cloud service-based applications, can be cost-effective and efficient. However, your organization typically doesn't have direct supervision or authority over the security controls implemented on external systems. For example, your organization is vulnerable to cyber attacks if employees are using their personal devices for work purposes and these devices have outdated or unpatched software or applications are in use without the proper permissions being assigned prior to employees' use of the app. Another example of this is when employees in your organization use Internet-based platforms to share files or conduct video calls, as these platforms are not controlled by your organization's IT security infrastructure or architecture. The less control you have over systems and devices that process, store, or transmit business information, the less confident you can be that the information is secure. It is recommended that your organization conduct a risk assessment and a supply chain assessment prior to sanctioning the use of personal devices, applications, or Internet and cloud-based systems for employee use. For more information on risk and supply chain risk assessments, see ITSG-33 [2] and *A* Cyber Supply Chain: An Approach to Assessing Risk (ITSAP.10.070) [11].

Before contracting potential service providers, such as CSPs, you should identify the data that will be accessible to the service provider and the sensitivity level of that data. By understanding your data and its sensitivity, you can identify the security controls that are required to protect it appropriately.

Data sensitivity is measured by the impact a compromise would have on your organization's ability to achieve its mandate. Data sensitivity is categorized as high, medium, or low:

- **High (H)**: Compromise has a critical or a prohibitive impact on your organization's ability to achieve its mandate;
- **Medium (M)**: Compromise has a major impact on your organization's ability to achieve its mandate; or

- **Low (L)**: Compromise has a moderate impact on your organization's ability to achieve its mandate.

Your organization is always responsible for protecting the confidentiality, integrity, and availability of your networks, systems, and information. To protect your systems from compromise, damage, or harm, you should only permit the use of an external system if you have verified that the system has security controls that are consistent with your security policies and plans. To verify the controls, you can, for example, use third-party, independent assessments or attestations. Choose a method that suits the confidence level required by your organization.

Your organization may determine that there's a higher level of risk associated with prohibiting the use of these devices; we recommend that you restrict the use of these devices in the following ways:

- ensure that approved security controls are implemented on devices before they can connect to organizational systems
- limit device access to certain types of information, services, or applications
- use virtualization techniques to limit processing and storage activities to your organization's servers or other system components
- ensure users agree to your organization's terms and conditions

When entering into an agreement with a CSP or managed service providers (MSPs), data storage should be discussed, and terms agreed upon. When data is stored outside of your organization's infrastructure, you need to know where it is going to be stored, for example the geographical location of the CSP's or MSP's data centre. The location of your data is important, as data stored outside of Canada is subject to different privacy, security, and data ownership laws and regulations. Depending on the industry or the sector to which your organization belongs, the data may also be subject to different regulations and standards that govern the data's retention, disclosure to third parties, and chain of custody. Ensure you document the terms of data residency in your service level agreement (SLA) with the CSP or MSP.

6.2 Document agreements (AC-20 and SA-9)

If using information systems that are owned, operated, or maintained by another organization or service provider, you should document all agreements with third parties. As an example, you should ensure that you have a SLA with CSPs. SLAs describe the level of service that you expect from the CSP. They also define expectations with regards to the performance of security controls, describe measurable outcomes, and identify remedies and response requirements for instances of non-compliance or security incidents. SLAs should be consistent with your organizational security policies and procedures. You should also review all agreements periodically.

Your organization and the service provider both have roles when it comes to protecting systems and data. Your organization is the data owner and is legally responsible for data security. Therefore, it is critical that you explicitly define your organization's security requirements and ask a CSP or MSP the right questions before you sign on to use a service. Having this information will ensure that you define an effective service level agreement with third-party service providers.

7 Set up compliance monitoring

To enforce your organization's security policies and ensure that external regulations are followed, you should have a compliance program. As an example, with a proper compliance monitoring framework, your organization can demonstrate that it handles sensitive information, such as personal information, appropriately.

You can also use your compliance monitoring program to identify and analyze risks and evaluate the effectiveness of your security controls. Your compliance monitoring framework can be used as a benchmark to ensure that risks are mitigated appropriately.

7.1 Continuous monitoring (AU-1)

You should ensure that all endpoint devices are monitored continuously. By monitoring devices, you can detect and follow up on uncharacteristic behaviour or suspected compromises.

Your organization's information systems should have audit logs to ensure that events (e.g. updates, changes, authentication attempts) are captured for future review. You should ensure that logs can only be accessed by authorized individuals. Keep in mind that if you have outsourced some services, then it can be more difficult to obtain the logs.

We also recommend using automated mechanisms, such as periodic scanning, to detect any unauthorized hardware, software, and firmware components within the information system. If unauthorized components are detected, you should disable their network access and isolate them (e.g. sandboxing).

8 Summary

One of our top 10 recommended IT security actions is to protect information at the enterprise level. The guidance included in this document is based on several of the security controls detailed in Annex 3A of ITSG-33 [2]. This document is not comprehensive or all-encompassing. To best protect information at the enterprise level, you should also review the other top 10 recommended IT security actions. You can refer to our other publications, such as ITSM.10.093 Top 10 IT Security Actions: Provide Tailored Cyber Security Training [12] or ITSM.10.094 Top 10 IT Security Actions: Manage Administrative Privileges [13].

Your organization's IT assets and information are valuable and enable your organization's continued operation. These assets are also a valuable target to threat actors. Your organization is always responsible for protecting the confidentiality, integrity, and availability of your networks, systems, and information. You should implement the security controls that address your organization's business and security requirements.

8.1 Contact information

For more information on implementing the guidance included in this document or any of our other 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

9 Supporting Content

9.1 List of abbreviations

Term	Definition
AC	Access control (security control family code)
AU	Audit and accountability (security control family code)
BYOD	Bring your own device
CM	Configuration management (security control family code)
COBO	Corporately owned and for business only
COPE	Corporately owned and personally enabled
CP	Contingency planning (security control family code)
CSP	Cloud Service Provider
CYOD	Choose your own device
IT	Information technology
MP	Media protection (security control family code)
MSP	Managed Service Provider
RA	Risk assessment (security control family code)
SA	Systems and service acquisition (security control family code)
SI	System and information integrity (security control family code)
SLA	Service Level Agreement
TRA	Threat and risk assessment

9.2 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.
Backdoor	The use of covert methods to bypass authentication requirements and access software and devices.
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

Term	Definition
	claims to be. Integrity also applied to business processes, software application logic, hardware, and personnel.
Information system	An integrated set of components for collecting, storing and processing data and providing information, knowledge, and digital products.
Information system component	An information system is made up of key components, including hardware, software, databases, networks, and people.
Insider threat	Any individual who has knowledge of or access to your organization's infrastructure and information and who uses, either knowingly or inadvertently, the infrastructure or information to cause harm.
IT asset	The components of an information system, including business applications, data, hardware, and software.
Malware	Malicious software (e.g. viruses, worms, Trojans, spyware, adware) designed to infiltrate or damage a computer system.
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).
Ransomware	A type of malware that denies a user's access to a system or data until a sum of money is paid to the threat actor.
Risk	The likelihood and the impact of a threat using a vulnerability to access an asset.
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.
Supply chain	The network and processes that exist between an organization and its suppliers to produce and distribute a product.
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.

9.3 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*. September 2021.
2	Canadian Centre for Cyber Security. *ITSG-33 IT Security Risk Management: A Lifecycle Approach*. December 2014.
3	Canadian Centre for Cyber Security. *Baseline Cyber Security Controls for Small and Medium Organizations*. Version 1.1. June 2019.

Number	Reference
4	Canadian Centre for Cyber Security. *ITSAP.10.003 How to Protect Your Organization from Insider Threats*. February 2020.
5	Canadian Centre for Cyber Security. *ITSAP.00.070 Supply Chain Security for Small and Medium Organizations*. March 2019.
6	Canadian Centre for Cyber Security. *ITSAP.40.001 Protecting High-Value Information: Tips for Small and Medium Organizations*. April 2019.
7	Canadian Centre for Cyber Security. *ITSAP.40.018 Guidance on Becoming Cryptographically Agile*. May 2022.
8	Canadian Centre for Cyber Security. *ITSAP.00.001 Using Your Mobile Device Securely*. October 2018.
9	Canadian Centre for Cyber Security. *ITSM.80.001 Securing the Enterprise for Mobility*. July 2016.
10	Canadian Centre for Cyber Security. *ITSM.70.003 End user security for Bring-Your-Own-Device (BYOD) deployment models*. May 2022.
11	Canadian Centre for Cyber Security. *ITSAP.10.070 Cyber supply chain: An approach to assessing risk*. July 2022.
12	Canadian Centre for Cyber Security. *ITSM.10.093 Top 10 IT Security Actions: Provide Tailored Cyber Security Training*. February 2020.
13	Canadian Centre for Cyber Security. *ITSM.10.094 Top 10 IT Security Actions: Managing and Controlling Administrative Privileges*. July 2022.

Annex A ITSG-33 security control catalogue

A.1 Technical security controls: access control

A.1.1 Access control

Table 2 lists the applicable access control security control, as defined in Annex 3A of ITSG-33 [2].

Table 2: ITSG-33 technical security controls: access control

Number	Control	Requirement	Control enhancements	Related ITSG-33 controls
AC-20	Use of external information systems	(A) The organization establishes terms and conditions that are consistent with any trust relationships established with other organizations that own, operate, and maintain external information systems, allowing authorized individuals to access the information system from external information systems. (B) The organization establishes terms and conditions that are consistent with any trust relationships established with other organizations that own, operate, and maintain external information systems, allowing authorized individuals to process, store, or transmit organization-controlled information using external information systems	**Limits on authorized use:** The organization permits authorized individuals to use an external information system to access the information system or to process, store, or transmit organization-controlled information only when the organization: i. Verifies the implementation of required security controls on the external system as specified in the organization's information security policy and security plans ii. Retains approved information system connection or processing agreements with the organizational entity hosting the external information system See Annex 3A of ITSG-33 for related control CA-2. **Portable storage devices:** The organization [*Select: restricts, prohibits*] the use of organization-controlled mobile devices by authorized individuals on external information systems.	AC-3 AC-17 AC-19 CA-2 CA-3 PL-4 SA-9

			Non-organizationally owned systems, components, and devices: The organization [*Select: restricts, prohibits*] the use of non-organizationally owned information systems, system components, or devices to process, store, or transmit organization information. **Network-accessible storage devices:** The organization prohibits the use of [*organization-defined network-accessible storage devices*] in external information systems.	

A.1.2 Audit and accountability

Table 3 lists the applicable audit and accountability security control, as defined in Annex 3A of ITSG-33 [2].

Table 3: ITSG-33 technical security controls: audit and accountability

Number	Control	Requirement	Control enhancements	Related ITSG-33 controls
AU-1	Audit and accountability policies and procedures	(A) The organization develops, documents, and disseminates to [*organization-defined personnel or roles*]: i. An audit and accountability policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. ii. Procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls. (B) The organization reviews and updates the current: i. Audit and accountability policy [*organization-defined frequency*]. ii. Audit and accountability procedures [*organization-defined frequency*].	None	

A.2 Operational security controls

A.2.1 Configuration management

Table 4 lists the applicable configuration management security control, as defined in Annex 3A of ITSG-33 [2].

Table 4: ITSG-33 operational security controls: configuration management

Number	Control	Requirement	Control enhancements	Related ITSG-33 controls
CM-8	Information system component inventory	(A) The organization develops and documents an inventory of information system components that accurately reflect the current information system. (B) The organization develops and documents an inventory of information system components that includes all components within the authorization boundary of the information system. (C) The organization develops and documents an inventory of information system components that is at the level of granularity deemed necessary for tracking and reporting. (D) The organization develops and documents an inventory of information system components that includes [*Assignment: organization-defined information deemed necessary to achieve effective information system component accountability*]. (E) The organization reviews and updates the information system component inventory [*Assignment: organization-defined frequency*].	**Updates during installations and removals:** The organization updates the inventory of information system components as an integral part of component installations, removals, and information system updates. **Automated maintenance:** The organization employs automated mechanisms to help maintain an up-to-date, complete, accurate, and readily available inventory of information system components. Also see Annex 3A of ITSG-33 for related control SI-7. **Automated unauthorized component detection:** i. The organization employs automated mechanisms [*Assignment: organization-defined frequency*] to detect the presence of unauthorized hardware, software, and firmware components within the information system ii. The organization takes the following actions when unauthorized components are detected: [Selection (one or more): disables network access by such components, isolates the components, notifies [Assignment: organization defined personnel or roles]. Also see Annex 3A of ITSG-33 for related controls AC-17, AC-18, AC-19, CA-7, SI-3, SI-4, SI-7, RA-5.	AC-17 AC-18 AC-19 CA-7 CM-2 CM-6 RA-5 SA-4 SI-3 SI-4 SI-7

			Accountability information: In the information system component inventory information, the organization includes a means for identifying by [*Selection (one or more): name, position, role*], the individuals who are responsible and accountable for administering those components. **No duplicate accounting of components:** The organization verifies that all components within the authorization boundary of the information system are not duplicated in other information system component inventories. **Assessed configurations and approved deviations:** The organization includes assessed component configurations and any approved deviations to current deployed configurations in the information system component inventory. Also see Annex 3A of ITSG-33 for related controls CM-2 and CM-6. **Centralized repository:** The organization provides a centralized repository for the inventory of information system components. **Automated location tracking:** The organization employs automated mechanisms to support tracking of information system components by geographic location. **Assignment of components to systems:** i. The organization assigns [*Assignment: organization-defined acquired information system components*] to an information system. ii. The organization receives an acknowledgement from the information system owner of this assignment. Also see Annex 3A of ITSG-33 for related control SA-4.	

A.2.2 Contingency planning

Table 5 lists the applicable contingency planning security control, as defined in Annex 3A of ITSG-33 [2].

Table 5: ITSG-33 operational security controls: contingency planning

Number	Control	Requirement	Control enhancements	Related ITSG-33 controls
CP-9	Information system backup	(A) The organization conducts backups of user-level information contained in the information system [*organization-defined frequency consistent with recovery time and recovery point objectives*]. (B) The organization conducts backups of system-level information contained in the information system [*organization-defined frequency consistent with recovery time and recovery point objectives*]. (C) The organization conducts backups of information system documentation including security-related documentation [*organization-defined frequency consistent with recovery time and recovery point objectives*]. (D) The organization protects the confidentiality, integrity, and availability of backup information at storage locations. (E) The organization determines retention periods for essential business information and archived backups.	**Testing for reliability and integrity:** The organization tests backup information [*organization-defined frequency*] to verify media reliability and information integrity. See related security control CP-4. **Test restoration using samplings:** The organization uses a sample of backup information in the restoration of selected information system functions as part of contingency plan testing. See related security control CP-4. **Separate storage for critical information:** The organization stores backup copies of [*organization-defined critical information system software and other security-related information*] in a separate facility or in a fire-rated container that is not collocated with the operational system. See related security controls CM-2 and CM-8. **Transfer to alternate storage site:** The organization transfers information system backup information to the alternate storage site [*organization-defined time period and transfer rate consistent with the recovery time and recovery point objectives*]. **Redundant secondary system:**	AC-3 CM-2 CM-8 CP-2 CP-4 CP-6 CP-7 CP-10 MP-2 MP-4 MP-5 SC-13

			The organization accomplishes information system backup by maintaining a redundant secondary system that is not collocated with the primary system and that can be activated without loss of information or disruption to operations. See related security controls CP-7 and CP-10. **Dual authorization:** The organization enforces dual authorization for the deletion or destruction of [*organization-defined backup information*]. See related security controls AC-3 and MP-2.	

A.2.3 Media protection

Table 6 lists the applicable media protection security control, as defined in Annex 3A of ITSG-33 [2].

Table 6: ITSG-33 operational security controls: media protection

Number	Control	Requirement	Control enhancements	Related ITSG-33 controls
MP-6	Media sanitization	(A) The organization sanitizes [*organization-defined information system media*] prior to disposal, release out of organizational control, or release for reuse, using [*organization-defined sanitization techniques and procedures*] in accordance with applicable GC and organizational standards and policies. (B) The organization employs sanitization mechanisms with the strength and integrity commensurate with the security category or classification of the information.	**Review, approve, track, document, and verify:** The organization reviews, approves, tracks, documents, and verifies media sanitization and disposal actions. See related security control SI-12. **Equipment testing:** The organization tests sanitization equipment and procedures [*organization-defined frequency*] to verify that the intended sanitization is being achieved. **Non-destructive techniques:** The organization applies non-destructive sanitization techniques to portable storage devices prior to connecting such devices to the information system under the following circumstances: [*organization-defined circumstances requiring sanitization of portable storage devices*]. See related security control SI-3. **Dual authorization:** The organization enforces dual authorization for the sanitization of [*organization-defined information system media*]. See related security controls AC-3 and MP-2. **Remote purging and wiping of information:** The organization provides the capability to purge/wipe information from [*organization-defined information systems, system components, or devices*] either remotely	AC-3 MA-2 MA-4 MP-2 RA-3 SC-4 SI-3 SI-12

			or under the following conditions: [*organization-defined conditions*].	
MP-7	Media Use	(A) The organization [*Select: restricts, prohibits* the use of [*organization-defined types of information system media*] on [*organization-defined information systems or system components*] using [*organization-defined security safeguards*]. Note: This control also applies to mobile devices with information storage capability (e.g. smart phones, tablets, e-readers).	**Prohibit use without owner:** The organization prohibits the use of portable storage devices in organizational information systems when such devices have no identifiable owner. See related control PL-4. **Prohibit use of sanitization-resistant media:** The organization prohibits the use of sanitization-resistant media in organizational information systems. See related control MP-6.	AC-19 MP-6 PL-4

A.2.4 System and information integrity

Table 7 lists the applicable system and information integrity security control, as defined in Annex 3A of ITSG-33 [2].

Table 7: ITSG-33 operational security controls: system and information integrity

Number	Control	Requirement	Control enhancements	Related ITSG-33 controls
SI-12	Information output handling and retention	(A) The organization handles and retains information within the information system and information output from the system in accordance with applicable GC legislation and TBS policies, directives, and standards.	None	AC-16 AU-5 AU-11 MP-2 MP-4

A.3 Management security controls

A.3.1 Risk assessment

Table 8 lists the applicable risk assessment security control, as defined in Annex 3A of ITSG-33 [2].

Table 8: ITSG-33 management controls: risk assessment

Number	Control	Requirement	Control enhancements	Related ITSG-33 controls
RA-2	Security categorization	(A) The organization categorizes information and the information system in accordance with applicable Government of Canada legislation and TBS. (B) The organization documents the security categorization results (including supporting rationale) in the security plan for the information system. (C) The organization ensures that the security categorization decision is reviewed and approved by the authorizing official or authorizing official's designated representative.	None	CM-8 MP-4 RA-3 SC-7

A.3.2 System and services acquisition

Table 9 lists the applicable system and services acquisition security control, as defined in Annex 3A of ITSG-33 [2].

Table 9: ITSG-33 management security controls: system and services acquisition

Number	Control	Requirement	Control enhancements	Related ITSG-33 controls
SA-9	External information system services	(D) The organization requires that providers of external information system services comply with organizational information security control requirements and use [*organization-defined security controls*] in accordance with the *TBS Security and Contracting Management Standard*. (E) The organization defines and documents government oversight and user roles and responsibilities regarding external information system services. (F) The organization uses [*organization-defined processes, methods, and techniques*] to monitor security control compliance by external service providers on an ongoing basis.	**Risk assessments and organizational approvals:** i. The organization conducts an organizational assessment of risk before acquiring or outsourcing dedicated information security services. ii. The organization ensures that the acquisition or outsourcing of dedicated information security services is approved by [*organization-defined personnel or roles*]. See related security controls CA-6 and RA-3. **Identification of functions, ports, protocols, and services:** The organization requires providers of [*organization-defined external information system services*] to identify the functions, ports, protocols, and other services required for the use of such services. See related control CM-7. **Establish and maintain trust relationship with providers:** The organization establishes, documents, and maintains trust relationships with external service providers based on [*organization-defined security requirements, properties, factors, or conditions defining acceptable trust relationships*].	CA-3 CA-6 CM-7 IR-7 PS-7 RA-3

			Consistent interests of consumers and providers: The organization uses [*organization-defined security safeguards*] to ensure that the interests of [*organization-defined external service providers*] are consistent with and reflect organizational interests. **Processing, storage, and service location:** The organization restricts the location of [*Select one or more: information processing, information/data, information system services*] to [*organization-defined locations*] based on [*organization-defined requirements or conditions*].	