Communications Security Establishment
Centre de la sécurité des télécommunications

CANADIAN CENTRE FOR CYBER SECURITY

Top 10 IT security actions: No. 3 managing and controlling administrative privileges

Management

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 Top 10 Information Technology Security Actions to Protect Internet-Connected Networks and Information (ITSM.10.089) [1][1].

Effective date

This publication takes effect on July 19, 2022.

Revision history

Revision	Amendments	Date
1	First release.	July 19, 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 enforce the management of administrative privileges. This document outlines some of the actions that your organization can take to manage and control administrative privileges. The guidance in this document is based on the security controls from ITSG-33 IT Security Risk Management: A Lifecycle Approach [2].

This document is part of a suite of documents that focuses on the top 10 IT security actions recommended in ITSM.10.089 [1]. Implementing all 10 of the recommended security actions can reduce your organization's vulnerability to cyber threats. However, 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:

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

D97-4/10-094-2022E-PDF
978-0-660-43806-1

Table of contents

List of figures

List of tables

List of annexes

1 Introduction

This document provides guidance on managing administrative privileges. Managing and controlling administrative privileges reduces your organization's exposure to cyber threats that could 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].

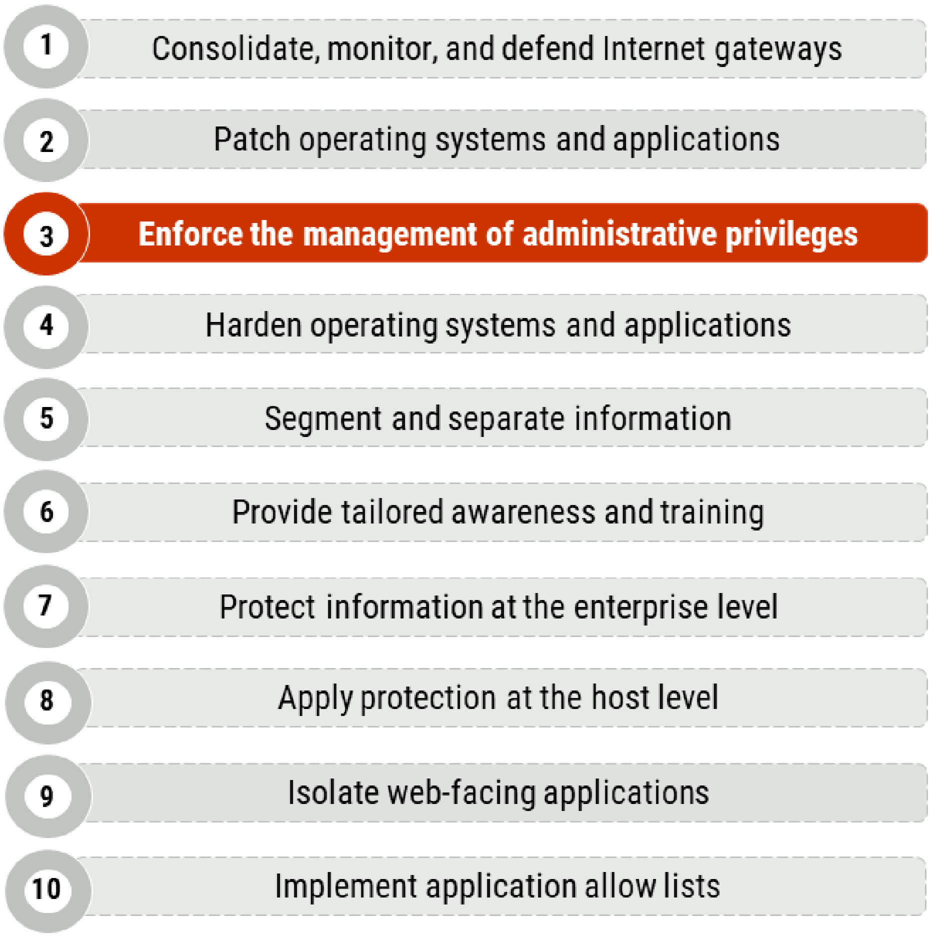
The guidance in this document is not comprehensive or all-encompassing. It only outlines some of the security controls that you can implement to protect your organization's information. Refer to Baseline Cyber Security Controls for Small and Medium Organizations [3] for more information on the security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



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 awareness and 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

1.2 IT security risk management process

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:

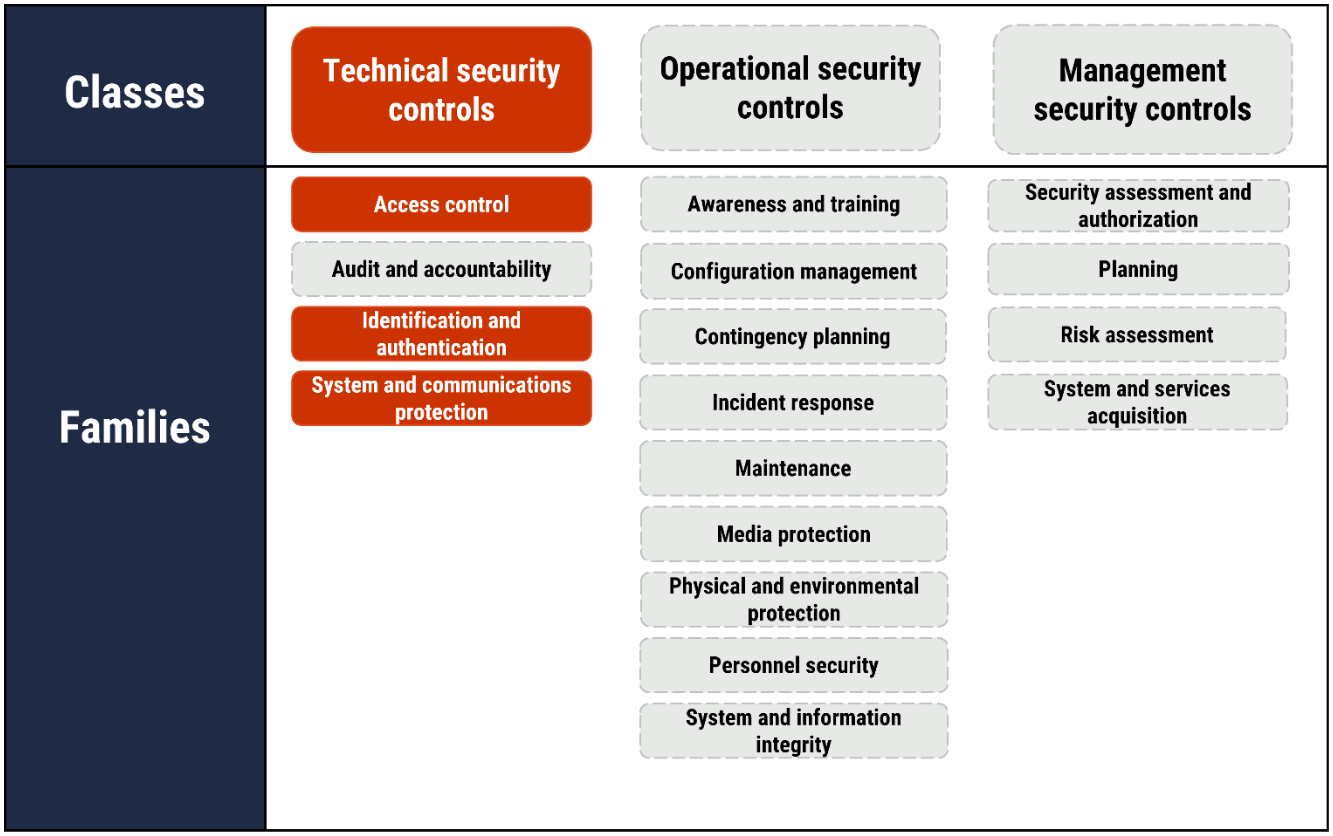
- **Technical security controls:** Security controls that are implemented and executed by information systems primarily through security mechanisms contained in hardware, software, and firmware components.
- **Operational security controls:** Information system security controls that are primarily implemented 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, this document includes some of the actions that fall under the Access Control (AC), Identification and Authentication (IA), and the System and Communication Protection (SC) control families. This document addresses the following controls:

- **AC-2 account management**
- **AC-6 least privilege**
- **AC-17 remote access**
- **IA-2 identification and authentication (organizational users)**
- **SC-3 security function isolation**.

See Annex A of this document for more information on controls AC-2, AC-6, AC-17, IA-2, and SC-3.

Figure 2: Applicable security control classes and families as described in ITSG-33



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	

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 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 Vulnerabilities and threats

Administrator accounts are high-value targets for threat actors. If threat actors gain access to these accounts, they can use the elevated privileges to affect your organization's operating environment, propagate their attacks (e.g. spread malware) through your entire network, and access sensitive information. Threat actors can also gain insight into the detection and remediation activities that are currently in place on your organization's systems. With this insight, threat actors can avoid detection and prevent you from mitigating their attacks.

External threat actors use different techniques, such as malware and phishing attacks, to compromise and gain entry to networks and systems. Compromises can result from normal user activity, such as opening emails or visiting websites. Threat actors may also exploit known vulnerabilities or use stolen credentials to access administrative accounts. Table 1 includes some examples of different attack methods.

Table 1: Examples of attack methods used

Attack method	Description
Malware	A threat actor uses malicious software to gain access to local or domain administrative accounts. For example, consider if a user checks email while signed on as an administrator and opens a malicious email attachment or visits a malicious website. The malicious file or exploit may contain executable code that runs on the user's machine. The threat actor can then take over the machine, install keystroke loggers or remote-control software to steal administrative credentials and 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 tools (e.g. a script or bot) to guess authentication credentials, including usernames, passwords, passphrases, or personal identification numbers (PINs). In a dictionary-based attack, a threat actor uses a list of commonly used passwords to guess the correct password.
Privilege escalation	A threat actor exploits a bug, design flaw, or configuration oversight in an operating system or software application to get privileged access and perform unauthorized actions.
Pass the hash	A threat actor exposes a user's authentication credentials on a compromised workstation. These credentials, which are usually hashed passwords, are passed around the network to help a threat actor move laterally through a network.

Once a threat actor has control of an initial endpoint (e.g. desktops, laptops, mobile devices, servers), the threat actor can begin the process of trying to gain access to other privileged account credentials, traversing multiple systems, and gaining access to data. Threat actors can also gain access to your data and systems in cloud-based services or infrastructure using similar methods as described for on-premises infrastructure. Threat actors want to stay on your networks and systems for as long as possible; they will try to hide their presence and activities (e.g. install rootkits to hide malicious files, delete applications, tamper with system and security event logs).

Threat actors are not only interested in gaining access to administrative accounts; they want to gain access to as many accounts as possible, even user accounts. Depending on your access control model, even user accounts may have access to critical, sensitive, or valuable data and systems. Users with administrative privileges can make configuration and operational changes to your organization's networks, systems, and devices. These users have greater access rights, which may include access to systems and devices on your organization's networks, as well as sensitive information (e.g. password hashes).

Managing administrative privileges in a cloud environment can expand the vulnerability and threat landscape. The roles and responsibilities of your organization and the cloud service provider (CSP) or managed service provider (MSP) will vary depending on the services you are consuming, as well as on your service and deployment model. Even when using cloud or managed services, your organization is still responsible and accountable for securing your data. When working with a CSP, your organization is responsible for managing access control. To further reduce risk, your organization should retain full control of your user credentials and associated authentication processes. If you have outsourced your IT services to an MSP, you should be aware of who needs to be a privileged user.

Restricting administrative privileges and managing access controls (e.g. authentication and authorization), whether on-premises, with a CSP or MSP, or a hybrid model, are mitigation strategies that can help protect your organization against threats. These mitigation strategies make it more difficult for threat actors to gain access to and misuse administrative privileges. These strategies also ensure that your users only have access to the systems and the information that they require to perform their job functions.

3 Authentication and authorization (IA-2, AC-6)

This section includes guidance on authenticating and authorizing administrative accounts and privileges. This guidance is based on security controls IA-2 and AC-6. For more information on these controls and other related security controls, see Annex A of this document and Annex 3A of ITSG-33 [2].

Access control, which is the selective restriction of a user's access to networks, systems, and data, consists of the following two elements:

- Authentication: A process or measure used to verify a user's identity; and
- Authorization: Access privileges granted to a user, program, or process.

Your organization should have user authentication policies in place that balance security with usability. Your organization's access control policy should persist when you use CSPs or MSPs, regardless of whether the data is stored on site or in the cloud. When using CSPs or MSPs your organization and the service provider must agree on the roles and responsibilities related to access control. You should ensure that all information systems identify and authenticate organizational users, or processes acting on behalf of users. You should also identify and authenticate the individuals and devices requiring access to information and the services you have hosted in the cloud to an acceptable level of assurance. The acceptable level of assurance is determined by your risk assessment. The authentication process can occur through the use of your device inventory, active directory, and other organizational identity access management (IAM) policies and procedures.

Single sign-on (SSO) is an approach that can be used to reduce the burden of authentication across multiple applications. In an SSO approach, users get a single identity, and a single set of credentials, that they can use with the software your organization uses. However, the compromise of an individual authenticator can allow threat actors to have wider system access, which is particularly risky for administrative accounts. Implementing multi-factor authentication (MFA), applying least privilege, and separating administrative functions from normal user functions can reduce the risk of using SSO for administrative accounts.

3.1 Implement multi-factor authentication (MFA)

You should use MFA for network and local access to administrative, privileged, and non-privileged accounts. MFA involves using credentials beyond usernames and passwords when logging into accounts; these additional credentials may include personal identification numbers (PINs), physical or digital tokens, smartcards, or biometrics. To add an additional layer of security to your accounts, MFA uses a combination of:

1. Something you know (e.g. a password, passphrase, PIN).
2. Something you have (e.g. a physical possession of a token, a smartcard).
3. Something you are (e.g. a biometric, like your fingerprint).

To count as MFA, you must use credentials that come from at least two of these three different categories (e.g. entering two passwords is not considered MFA).

If your organization is currently or plans to work with a CSP, ensure the applications offered by the cloud infrastructure or CSP support MFA. You should also apply MFA to cloud portal service administration accounts and any associated recovery accounts. It is also important to ensure that all cloud service accounts, including cloud portal service administration and recovery accounts, use different passwords and authentication factors than those used within the organization's on-premises infrastructure.

Threat actors continue to evolve their attack methods. They can use methods like brute force, keylogging, phishing, and social engineering to steal passwords. MFA is the most effective countermeasure for password theft attacks.

For more information on passphrases and complex passwords, see Best Practices for Passphrases and Passwords (ITSAP.30.032) [4] and Steps for Effectively Deploying Multi-Factor Authentication (MFA) (ITSAP.00.015) [5].

3.2 Apply the principle of least privilege

Least privilege is the principle of giving users only the set of privileges that they need to perform authorized tasks. This principle limits the damage that can result from accidental, incorrect, or unauthorized access and use of systems and information.

Administrative functions should be restricted to only those who require that level of privilege. You may want to consider creating additional processes, roles, and information system accounts as necessary to maintain least privilege. You can assign user privileges more specifically by using separate processing domains. For example, you can use virtualization techniques to allow a user to have additional privileges when using a virtual machine and limited privileges when using other environments.

Consider the following key questions when assigning administrative privileges to employees:

- What tasks absolutely require administrative privileges and how many employees are needed to complete these tasks?
- How are administrative activities logged and who is responsible for reviewing and auditing these activity logs?
- Are adequate security protections in place to manage and control these administrative privileges?

The access control model that you choose to implement depends on the type and the sensitivity of the data that your organization handles and processes. Implementing data classification and assigning access based on these classifications can assist in managing access and maintaining least privilege. Role-based access control (RBAC) could also be considered as an access control model. RBAC maps user access rights to their role within the organization. Many CSPs offer data classification and access control model provisioning capabilities as part of their out-of-the-box service packages. If your organization has a hybrid cloud and on-premises model, there are also third-party companies that will work with your IT staff to classify data within your local and remote repositories.

4 Administrative account management (AC-2, AC-17(100) SC-3)

This section includes guidance on managing administrative accounts and privileges that are applicable whether your organization employs an on-premises, cloud, or a hybrid model. This guidance is based on security controls AC-2, AC-17(100), and SC-3. For more information on these controls, and other related controls, see Annex A of this document and Annex 3A of ITSG-33 [2].

By managing and controlling administrative accounts and privileges, your organization creates an operating environment that is stable, predictable, and easier to administer and support. Proper access control and account management means that fewer users can make significant changes to the operating environment. You can also ensure that your network administration and support is simplified.

When you manage administrative accounts and privileges, you also make it more difficult for threat actors to compromise your networks and systems. Threat actors target these accounts to attempt to propagate their attacks (e.g. spreading malware, escalating privileges) throughout an entire network and access sensitive information.

4.1 Separate administrative functions and workstations

Compromises can result from normal user activity, such as opening emails or visiting websites. Your organization puts itself at greater risk if your users can access email services and websites while logged in to their administrative accounts. There is no need for any user to have one account with both normal user access to networks, such as the Internet and email services, and administrative privileges. Users with administrative privileges should have a separate administrative account, with separate credentials, despite your organization's cloud, on-prem, or hybrid environment.

To identify and separate administrative functions from non-administrative functions, you should consider the following:

- User roles that require access to sensitive data (including your CSP and MSP users);
- Responsibilities, accountabilities, and tasks for each user role;
- Tasks that absolutely require administrative privileges;
- Users who are required, and who are authorized, to carry out administrator tasks; and
- Time frame (i.e. permanently or for a predetermined length of time) in which users need to carry out administrator tasks (e.g. permanent tasks, emergency tasks).

We strongly recommend that you create separate administrative accounts for users who require them. Ensure that these administrative accounts do not have the ability to access the Internet or email services, as this can expose your organization unnecessarily to threat actors. Ensure that administrative tasks are performed on dedicated administrative computers that cannot access the Internet or email services. For remote access, Annex 3A of ITSG-33 [2] under AC-17(100) states that remote access to privileged accounts should be performed on dedicated management consoles governed entirely by the system's security policies and used exclusively for this purpose (e.g. Internet access not allowed). For cloud administration from this dedicated workstation, ensure it requires a VPN or allow lists to access the cloud tenancy.

Your organization should create and maintain an inventory of all its administrative accounts, including domain and local accounts. You may wish to implement restrictions (e.g. time of day, day of week, log in location) for administrative accounts in an on-prem environment. It is important to note there could be instances where these restrictions can inhibit your ability to perform actions, such as in response to an incident that falls outside of the designated time of day or location restrictions in place.

Whatever restrictions you apply to the management of organizational administrative accounts and privileges should be reflected in your service level agreement with your MSP as they should be held to the same policies and restrictions.

4.2 Implement two person integrity (TPI) and dual authorization for administrative accounts

Validating and verifying sensitive administrative tasks related to highly sensitive data or critical systems can help protect your organization's environment. Your organization can achieve this by implementing TPI and dual authorization.

TPI requires at least two authorized individuals to access or perform a critical task at the same time. This reduces the risk of sensitive information or processes being accessed by stolen credentials. TPI also ensures that the sensitive area can only be accessed on a need-to-know basis. An example of TPI applied at the administrator access level includes the use of a two-key system. Both administrators would be provided with a key and both keys would be required to perform or complete a task.

Dual authorization ensures that sensitive tasks or administrative operations performed on systems requires approval from at least two authorized individuals before system changes are applied.

Another use case that your organization could implement is a form of TPI when releasing credentials to users. An administrator can provide the user with half the password or passphrase they require to log into the environment, with the other half being provided to someone who can authenticate the user, like the user’s manager. In this method, there is not one user with immediate access to critical systems or data and an authentication process must be completed by a second user in order to allow the access to be granted.

For more information on securing remote access, see Security Tips for Organizations with Remote Workers (ITSAP.10.016) [6].

4.3 Log and monitor privileged accounts

Your organization is responsible for specifying the conditions or circumstances under which administrative and privileged accounts can be used (e.g. certain times of day or days of the week, for specific durations of time). Information systems should have audit logs that detail the actions (e.g. making system changes, logging in and out of accounts) taken by privileged accounts. For attribution purposes, all administrative accounts should be linked to an identifiable individual.

We recommend that you configure your information systems to log any changes made to an administrative account (e.g. when an account is added or removed). Your system logs should also include unsuccessful account log-in attempts. Logged events and actions should include date and time stamps.

If your organization is working with a CSP or MSP, you should ensure there is continuous monitoring of system events and performance. The CSP or MSP should provide you with regular audit logs that include access reports for all administrative accounts [7].

You can use your system logs and CSP or MSP provided logs to establish a baseline of normal administrative and privileged user behaviour. You should review the audit logs regularly to detect any unusual behaviour. Be sure to have a schedule in place that determines how often the logs and audit information are reviewed.

Ensure all audit information (e.g. audit records, reports) is collected and retained. If possible, you should store audit information in a physically separate system or tamper-resistant repository.

4.4 Delete accounts and remove privileged access

Your organization's need for certain assigned administrative accounts and user privileges can change, and users may change job functions or leave your organization. You should review all user accounts regularly, especially administrative accounts and privileges, to validate that they are still required by the assigned users. When reviewing these accounts and privileges, determine whether any need to be reassigned or removed based on your business needs and security requirements. This review should also include accounts and privileges held by your CSP or MSP and should be included as requirements in your service agreements.

Keep in mind that emergency and temporary accounts are different from infrequently used accounts (e.g. local accounts used for special tasks defined by organizations or when network resources are unavailable). Such accounts remain available and are not subject to automatic disabling or removal dates. Conditions for disabling or deactivating accounts include the following examples:

- When shared, group, emergency, or temporary accounts are no longer required;
- When employees, or contractors, leave the organization; and
- When employees, or contractors, are transferred or terminated from the organization.

You should determine the period in which inactive accounts are disabled.

5 Summary

One of our top 10 recommended IT security actions is to manage and control administrative privileges. This document outlines our recommended best practices for protecting your organization’s administrative accounts and privileges from compromises, whether you employ an on-premises, cloud, MSP, or hybrid model. When assigning administrator accounts or privileged access to employees, keep the following considerations in mind:

- Create separate non-administrative accounts that are used to carry out non-administrative functions (e.g. checking email);
- Use strong authentication methods:
    - Use a unique password or passphrase for each privileged account;
    - Change default passwords for applications and devices;
    - Authenticate users before they are granted access to applications or devices; and
    - Use MFA;
- Ensure that unique, identifiable accounts are linked to individual users (i.e. attribution);
- Provide training to cover expected behaviours for users who have privileged accounts (e.g. log out of privileged accounts when they are not in use); and
- Remove or disable special access privileges when a user no longer requires them.

These best practices are based on the security controls detailed in Annex A of this documents and Annex 3A of ITSG-33 [2]. Effectively managing privileged accounts and access rights helps prevent threat actors from gaining control of privileged accounts and propagating exploits across your network or your systems and data stored in the cloud. Depending on the size of your organization, it may be difficult to properly secure every aspect of your IT infrastructure. However, you can focus your efforts on privileged accounts that, if compromised, put your organization at greater risk.

Managing privileged accounts 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]. Some additional measures that your organization should take include educating employees on cyber security, protecting endpoint devices by applying patches or implementing an application allow list, and isolating web-facing applications.

5.1 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

6 Supporting content

6.1 List of abbreviations

Term	Definition
AC	Access control (security control family)
CSP	Cloud service provider
GC	Government of Canada
IA	Identification and authentication (security control family)
IAM	Identity and access management
IT	Information technology
MFA	Multi-factor authentication
MSP	Managed service provider
PIN	Personal identification number
RBAC	Rule-based access control
SC	System communication protection (security control family)
SSO	Single sign-on

6.2 Glossary

Term	Definition
Access control	Certifying that only authorized access is given to assets (both physical and electronic). For physical assets, access control may be required for a facility or restricted area (e.g. screening visitors and materials at entry points, escorting visitors). For IT assets, access controls may be required for networks, systems, and information (e.g. restricting users on specific systems, limiting account privileges).
Authentication	A process or measure used to verify a user's identity.
Authorization	Access privileges granted to a user, program, or process.
Availability	The ability for the right people to access the right information or systems when needed. Availability is applied to information assets, software, and hardware (infrastructure and its components). Implied in its definition is that availability includes the protection of assets from unauthorized access and compromise.
Confidentiality	The ability to protect sensitive information from being accessed by unauthorized people.
Cyber attack	The use of electronic means to interrupt, manipulate, destroy, or gain unauthorized access to a computer system, network, or device.
Default account	The generic user permissions, which are usually administrative access rights, and passwords that are provided as the standard for applications and hardware. The default account is used during the initial set-up of applications and hardware.
Defence in depth	An IT security concept (also known as the Castle Approach) in which multiple layers of security are used to protect the integrity of information. These layers can include antivirus and antispyware software, firewalls, hierarchical passwords, intrusion detection, and biometric identification.

Term	Definition
Endpoint	A remote computing device (e.g. laptop, desktop, mobile phone) that communicates with a network to which it is connected.
Hash	A mathematical function that is used to convert a block or group of data into a fixed-length value, which is usually shorter than the original data. Hashes mask the original data with another value that can only be decoded by looking up the value from a hash table.
Integrity	The ability to protect 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.
Malware	Malicious software designed to infiltrate or damage a computer system, without the owner's consent. Common forms of malware include computer viruses, ransomware, spyware, and adware.
Management security control	A security control that focuses on the management of IT security and IT security risks.
Operational security control	A security control primarily implemented and executed by people and typically supported by the use of technology (e.g. supporting software).
Phishing	An attempt by a third party to solicit confidential information from an individual, group, or organization by mimicking or spoofing a specific, usually well-known brand, usually for financial gain. Phishers attempt to trick users into disclosing personal data, such as credit card numbers, online banking credentials, and other sensitive information, which they may then use to commit fraudulent acts.
Ransomware	A type of malware that denies a user's access to a system or data until a sum of money is paid.
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.
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.

6.3 References

Number	Reference
1	Canadian Centre for Cyber Security. ITSM.10.089 Top 10 IT 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. November 2012.
3	Canadian Centre for Cyber Security. Baseline Cyber Security Controls for Small and Medium Organizations. V1.1. June 2019.
4	Canadian Centre for Cyber Security. ITSAP.30.032 Best Practices for Passphrases and Passwords. September 2019.
5	Canadian Centre for Cyber Security. Steps for Effectively Deploying Multi-Factor Authentication (MFA) (ITSAP.00.015). May 2023.
6	Canadian Centre for Cyber Security. Security Tips for Organizations with Remote Workers (ITSAP.10.016). May 2020.
7	Government of Canada. GC Cloud Guardrails.

Annex A ITSG-33 security control catalogue

A.1 Technical security controls: Access control

Table 2 describes controls **AC-2 Account Management** and **AC-6 Least Privilege**, as defined in Annex 3A of ITSG-33 [2].

Table 2: ITSG-33 technical security controls: AC-2, A-6 and AC-17(100)

Number	Control	Requirement	Control enhancements	Related ITSG-33 controls
AC-2	Account Management	(A) The organization identifies and selects the following types of information system accounts to support organizational missions/business functions: [*organization-defined information system account types*]. (B) The organization assigns account managers for information system accounts. (C) The organization establishes conditions for group and role membership. (D) The organization specifies authorized users of the information system, group and role membership, and access authorizations (i.e. privileges), and other attributes (as required) for each account. (E) The organization requires approvals by [*organization-defined personnel or roles*] for requests to create information system accounts. (F) The organization creates, enables, modifies, disables, and removes information system	**Automated system account management:** The organization uses automated mechanisms to support the management of information system accounts. **Removal of temporary and emergency accounts:** The information system automatically [*Selection: removes, disables*] temporary and emergency accounts after [*organization-defined time period for each type of account*]. **Disable inactive accounts:** The information system automatically disables inactive accounts after [*organization-defined time period*]. **Automated audit actions:** The information system automatically audits account creation, modification, enabling, disabling, and removal actions, and notifies [*organization-defined personnel or roles*]. See related controls AU-2 and AU-12.	AC-3 AC-4 AC-5 AC-6 AC-10 AC-17 AC-19 AC-20 AU-9 IA-2 IA-4 IA-5 IA-8 CM-5 CM-6 CM-11 MA-3 MA-4 MA-5 PL-4 SC-13

Number	Control	Requirement	Control enhancements	Related ITSG-33 controls
		accounts according with [*organization-defined procedures or conditions*]. (G) The organization monitors the use of information system accounts. (H) The organization notifies account manager when: i. Accounts are no longer required. ii. Users are terminated or transferred. iii. Individual information system usage or need-to-know changes. (I) The organization authorizes access to the information system based on: i. A valid access authorization. ii. Intended system usage. iii. Other attributes as required by the organization or associated missions/business functions. (J) The organization reviews accounts for compliance with account management requirements [*organization-defined frequency*]. (K) The organization establishes a process for reissuing shared/group account credentials (if deployed) when individuals are removed from the group.	**Inactivity logout:** The organization requires that users log out when [*organization-defined time period of expected inactivity or description of when to log out*]. See related control SC-23. **Dynamic privilege management:** The organization system implements the following dynamic privilege management capabilities: [*organization-defined list of dynamic privilege management capabilities*]. See related control AC-16. **Role-based schemes:** i. The organization establishes and administers privileged user accounts according with a role-based access scheme that organizes allowed information system access and privileges into roles. ii. The organization monitors privileged roles assignments. iii. The organization takes [*organization-defined actions*] when privileged role assignments are no longer appropriate. **Dynamic account creation:** The information system creates [*organization-defined information system accounts*] dynamically. See related control AC-16.	

Number	Control	Requirement	Control enhancements	Related ITSG-33 controls
			Restrictions on use of shared groups and accounts: The organization only permits the use of shared and group accounts that meet [*organization-defined conditions for establishing shared and group accounts*]. **Shared and group account credential termination:** The information system terminates shared and group account credentials when members leave the group. **Usage conditions:** The information system enforces [*organization-defined circumstances and usage conditions*] for [*organization-defined information system accounts*]. **Account monitoring and atypical usage:** i. The organization monitors information system accounts for [*organization-defined atypical use*]. ii. The organization reports atypical use of information system accounts to [*organization-defined personnel or roles*]. See related control CA-7. **Disable accounts for high-risk individuals:** The organization disables accounts of users posing a significant risk within [*organization-defined time period*] of discovery of the risk.	

Number	Control	Requirement	Control enhancements	Related ITSG-33 controls
AC-6	Least Privilege	(A) The organization applies the principle of least privilege, allowing users (or processes acting on behalf of users) only the access necessary to accomplish assigned tasks according to organizational missions and business functions.	**Separate processing domains:** The information system provides separate processing domains to enable finer-grained allocation of user privileges. See related control AC-4, SC-3, SC-30, and SC-32.	AC-2 AC-3 AC-5 CM-6 CM-7 PL-2
AC-17	Remote Access	(A) The organization establishes and documents usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed. (B) The organization authorizes remote access to the information system prior to allowing such connections.	Remote access to privileged accounts is performed on dedicated management consoles governed entirely by the system's security policies and used exclusively for this purpose (e.g. Internet access not allowed).	N/A

A.2 Technical security controls: Identification and authentication

Table 3 describes controls **IA-2 Identification and Authentication (Organizational Users)**, as defined in Annex 3A of ITSG-33 [2].

Table 3: ITSG-33 technical security controls: IA-2

Number	Control	Requirement	Control enhancements	Related ITSG-33 controls
IA-2	Identification and Authentication (Organizational Users)	(A) The information system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users).	**Network access to privileged accounts:** The information system implements multi-factor authentication for network access to privileged accounts. See related control AC-6. **Network access to non-privileged accounts:** The information system implements multi-factor authentication for network access to non-privileged accounts. **Local access to privileged accounts:** The information system implements multi-factor authentication for local access to privileged accounts. See related control AC-6. **Local access to non-privileged accounts:** The information system implements multi-factor authentication for local access to non-privileged accounts.	AC-2 AC-3 AC-14 AC-17 AC-18 IA-4 IA-5 IA-8

Number	Control	Requirement	Control enhancements	Related ITSG-33 controls
			Group authentication: The organization requires individuals to be authenticated with an individual authenticator when a group authenticator is employed. **Network access to privileged accounts – separate device:** The information system implements multi-factor authentication for network access to privileged accounts such that one of the factors is provided by a device separate from the system gaining access and the device meets [*organization-defined strength of mechanism requirements*]. See related control AC-6. **Network access to non-privileged accounts – replay resistant:** The information system implements replay-resistant authentication mechanisms for network access to privileged accounts. **Single sign-on**: The information system provides a single sign-on capability for [*organization-defined list of information system accounts and services*].	

Number	Control	Requirement	Control enhancements	Related ITSG-33 controls
			Remote access – separate device: The information system implements multi-factor authentication for remote access to privileged and non-privileged accounts. One of the factors is provided by a device separate from the system being accessed. The device meets [*organization-defined strength of mechanism requirements*]. See related control AC-6. **Acceptance of personal identity verification (PIV) credentials:** The information system accepts and electronically verifies PIV credentials. See related controls AU-2, PE-3, SA-4. **Out-of-band authentication:** The information system implements [*organization-defined out-of-band authentication*] under [*organization-defined conditions*]. See related controls IA-10, IA-11, and SC-37.	

A.3 Technical security controls: System and communication protection

Table 4 describes controls **SC-3 Security Function Isolation**, as defined in Annex 3A of ITSG-33 [2].

Table 4: ITSG-33 technical security controls: SC-3

Number	Control	Requirement	Control enhancements	Related ITSG-33 controls
SC-3	Security Function Isolation	(A) The information system isolates security functions from non-security functions.	**Hardware separation:** The information system uses underlying hardware separation mechanisms to implement security function isolation. **Access and flow control functions:** The information system isolates security functions enforcing access and information flow control from non-security functions and from other security functions. **Minimize non-security functionality:** The organization minimizes the number of non-security functions included with the isolation boundary containing security functions. **Module coupling and cohesiveness:** The organization implements security functions as largely independent modules that maximize internal cohesiveness within modules and minimize coupling between modules.	AC-3 AC-6 SA-4 SA-5 SA-8 SA-13 SC-2 SC-7 SC-39

Number	Control	Requirement	Control enhancements	Related ITSG-33 controls
			Layered structures: The organization implements security functions as a layered structure minimizing interactions between layers of the design and avoiding any dependence by lower layers on the functionality or correctness of higher layers.	