Communications Security Establishment
Centre de la sécurité des télécommunications

CANADIAN CENTRE FOR CYBER SECURITY

Top 10 IT security actions: No. 9 isolate web-facing applications

MANAGEMENT

Canada

Foreword

ITSM.10.0-99 Top 10 IT Security Actions: No. 9 Isolate Web-Facing Applications is an UNCLASSIFIED publication issued under the authority of the Head of the Canadian Centre for Cyber Security (Cyber Centre). It's part of a suite of documents that focuses on the top 10 security actions recommended by the Cyber Centre in ITSM.10.189 Top 10 IT Security Actions to Protect Internet Connected Networks and Information [1][1]. For more information, email, or phone our Contact Centre:

Contact Centre

contact@cyber.gc.ca

(613) 949-7048 or 1-833-CYBER-88

Effective date

This publication takes effect on Month XX, 2022.

Revision history

Revision	Amendments	Date
1	First release.	Month XX, 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 isolate web-facing applications. A web-facing application is any program that can be accessed over the Internet and that uses web technology and browsers to perform tasks. Examples include email services, word processors, online file converters, and calendars. Web-facing applications can also include Internet of things (IoT) devices, such as security cameras and smart thermostats. The data you enter on these applications can be stored in an on-premises, cloud, or hybrid environment, and while it's accessible when you need it, it can also put your organization as risk of cyber attacks.

This document outlines several best practices for isolating web-facing applications to ensure that your organizational networks and systems are protected against common cyber threats. Isolating web-facing applications is part of a defence-in-depth protection strategy. The guidance in this document is based on the security controls found in ITSG-33 IT Security Risk Management: A Lifecycle Approach [2].

By isolating web-facing applications, you can reduce your exposure to common threats and protect your organization's systems and networks. This document focuses on specific security controls that can be used to isolate web-facing applications. To best protect your organization against cyber security threats that impact web-facing applications, your organization should implement additional security measures.

This document is part of a suite of documents that focuses on the top 10 IT security actions recommended in ITSM.10.189 [1]. While implementing all 10 of the recommended security actions can reduce your organization's vulnerability to cyber threats, you should review your current cyber security activities to determine whether additional actions are required. For more information on implementing the top 10 IT security actions, email or phone our Contact Centre:

Contact Centre

contact@cyber.gc.ca

(613) 949-7048 or 1-833-CYBER-88

Table of contents

List of figures

List of tables

List of annexes

1 IT security risk management: An overview

1.1 Top 10 IT security actions

This document provides guidance on isolating web-facing applications by using virtualization technology. Isolating these applications reduces your organization's exposure to common cyber threats that impact web-facing applications and that could compromise your networks, systems, and IT assets. This guidance is based on the advice in ITSM.10.189 [1] and the security controls listed in Annex 3A of ITSG-33 [2].

Our top 10 recommended IT security actions, which are listed in Figure 1 below and ITSM.10.189 [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.

Cyber security threats can have varying impacts based on your organization's business and technical environment. 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. 9 isolate web-facing applications

1.2 Relationship to the 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 (standardized security requirements to protect the confidentiality, integrity, and availability of IT assets). These security controls are divided into the following three classes, which are further divided into several families (or groupings) of related security controls:

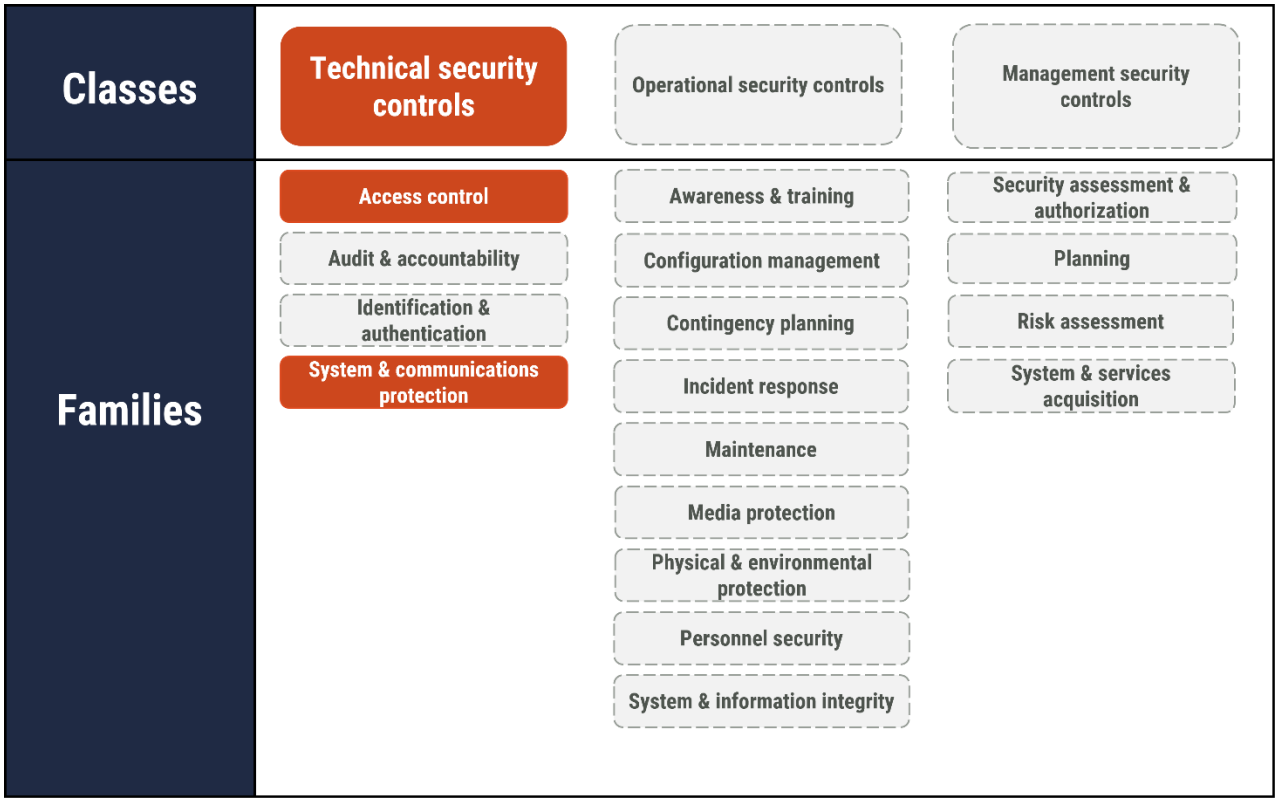
- **Technical security controls:** Security controls that are implemented and executed by information systems primarily through security mechanisms contained in hardware, software, and firmware components.
- **Operational security controls:** Information system security controls that are primarily implemented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

As illustrated in Figure 2, this document includes actions that fall under the access control (AC) and the system communication protection (SC) control families. This document addresses the following controls:

- **AC-6 Least Privilege**
- **SC-32 Information System Partitioning**

See Annex A of this document for more information on controls AC-6 and SC-32.

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



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

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

Note: The security controls and best practices in this document are not described in depth. As with any IT solution, your organization is responsible for reviewing its business and security requirements to determine how best to tailor your approach to security.

2 Threats to web-facing applications

This section provides an overview of the common threats to web-facing applications. Isolating all web-facing applications is one of the essential actions that you can take to reduce your organization's exposure to cyber threats.

A web-facing application is any program that can be accessed over a network connection and uses web technology and browsers to perform tasks over the Internet, such as email, word processors, file conversion, e-commerce, calendars, or IoT devices. Web applications are convenient and cost-effective. Data can be stored on-premises, in the cloud, or in a hybrid environment, which makes the information accessible when needed. Web-facing applications can be used to improve business processes and support remote work. Generally, web applications are easy to install and maintain because patches and updates can be rolled out remotely to devices.

However, when applications are developed, security is often an afterthought. If security measures aren't built into applications, they can be vulnerable to unauthorized access, data leaks, and other security issues. Code flaws and defects can also leave applications vulnerable to attacks, such as cross-site scripting (XSS) and structured query language (SQL) injection attacks.

2.1 Understand the common threats

Cyber threat actors look for ways to modify application parameters and execute unauthorized or malicious functionalities on applications. By exploiting application vulnerabilities, a threat actor can gain unauthorized access to sensitive information, like personal or business information, that is processed by and stored on web-facing applications. Attacks on web-facing applications can result in information exposure, identity theft, compromise of the application itself or other organizational systems, or denial of service.

Table 1 lists some examples of common threats to web-facing applications, including the method of attack and the potential impact the attack could have on your organization and on users of the application. The data in Table 1 is derived from the Open Web Application Security Project (OWASP) Top 10 Web Application Security Risks [3]. Note that this list of threats is not exhaustive.

Table 1: Common threats to web-facing applications

Threat	Method	Potential impact
Broken access control	Threat actors exploit vulnerabilities in access control enforcement, such as least privilege not being implemented or administrator rights not being reviewed and modified where needed. Common attack vectors include violation of the principle of least privilege or deny by default, parameter tampering or forced browsing (bypassing access control checks by modifying the URL or HTML page), and metadata manipulation.	Access control enforces policy such that users cannot act outside of their intended permissions. Failures typically lead to unauthorized information disclosure, modification or destruction of all data, or performing a business function outside the user's limits.

Threat	Method	Potential impact
Cross-site scripting (XSS)	Threat actors inject malicious script into a benign and trusted web application. The threat actor uses the application to send malicious code, usually in the form of browser-side scripts, to anyone who uses the application.	User's device becomes infected with malicious code that can access cookies, session tokens, or other sensitive information retained by the application.
Structured query language (SQL) injection	Threat actors add SQL code into the input data to affect the execution of predefined SQL commands.	Sensitive data may be deleted, changed, or revealed to the threat actor. A threat actor can also execute administration operations.
Command injection flaws	Attacks that use flaws which allow threat actors to relay malicious code through a web application to another system.	The threat actor can take control of the application.
Buffer overflows	A threat actor sends large amounts of data, which exceed the quantities that an application expects, causing the application to abandon normal behaviour.	The threat actor can execute commands or programs and gain access to systems.
Brute force attacks	A threat actor uses a trial-and-error method to gain access by guessing authentication information and subsequently to get information from the accessed account. A threat actor may use automated software to generate many consecutive guesses in the hopes that one is correct.	A threat actor gains access to a user's account and any sensitive information associated with the account (e.g. stored credit card information).
Path traversal	Threat actors use this attack, which is also referred to as directory traversal, to access files and directories stored outside the web root folder. A threat actor uses variables, such as dot-dot-slash ("../") sequences, to move up the directory hierarchy.	A threat actor can access application source code, user credentials, databases, or configuration and critical system files.
File inclusion vulnerability	A threat actor controls which file is executed at run time by using a variable to build a path to executable code. This attack usually affects applications that rely on a scripting run time.	A threat actor can use remote code execution to run an application or create a web shell on the web server, which can be used to run commands interactively from a remote location.
Server-side request forgery (SSRF)	Attacks that exploit a web application that is acquiring a remote resource without validating the user-supplied	Your systems can be targeted even if they are behind firewalls or

Threat	Method	Potential impact
	URL. Threat actors can coerce the application to send a crafted request to an unexpected destination, even when protected by a firewall, VPN, or another type of network access control list (ACL).	network ACLs. Since most modern web applications provide end users with convenient features, fetching a URL becomes a common scenario. They could scan to find open ports, access sensitive data, access the metadata storage of cloud services, or conduct a denial of service (DoS) attack. The severity of SSRF is becoming higher due to cloud services and the complexity of architectures.

3 Security controls for web-facing applications

This section introduces actions that your organization can take when isolating web-facing applications. These actions are based on security controls, **SC-32 Information System Partitioning** and **AC-6 Least Privilege**. For more information on these controls, see annexes A.1 and A.2 in this document.

Although the security controls described below are a good start to protecting your organization, you should also consider taking the following actions:

- Scan and test applications for vulnerabilities
- Update and patch applications as soon as updates and patches are available
- Implement an application allow list
- Implement web application firewalls
    - There are two different types of application firewalls: network-based application firewalls and host-based application firewalls. Both provide a barrier which protects local system resources from being accessed from the outside.

For more information on the above measures, see ITSM.10.095 Top 10 IT Security Actions: No. 10 Implement Application Allow Lists [4] and ITSM.10.096 Top 10 IT Security Actions: No. 2 Patch Operating Systems and Applications [5].

3.1 Information system partitioning (SC-32)

Your organization should isolate web-facing applications so that they reside in separate domains or environments to reduce the risk of back-end networks and information systems being compromised. Isolated applications are restricted or prohibited from accessing the network or communicating with other information system components. If an isolated application is infected with malware or compromised, the exploit will be contained and won't be able to spread beyond the isolated environment, known as a sandbox, to infect other hosts and systems.

Segmenting your networks into security zones enables you to isolate web-facing applications and protect your organization's systems and data. Segmentation reduces your organization's exposure to threats that could exploit publicly known vulnerabilities and compromise your networks, systems, and IT assets.

Network segmentation refers to a networking technique that divides a network into smaller, distinct subnetworks (subnets), enabling organizations to compartmentalize and deliver unique security controls and services to each subnet. Network security zones are logical groupings based on the underlying implementation of network segmentation. The unique security controls protecting a zone are defined within the zone interface point (ZIP).

A ZIP is a system that controls the flow of information between two zones. The differentiation between zones is called the boundary. The boundary contains ZIPs which are the only connecting points between zones. All data communication between zones must be through a ZIP which exclusively connects these two zones and creates a distinct communication path.

A cloud ZIP is used to describe the controlled interface connecting two zones. In a cloud environment, there are other logical segmentation mechanisms which may not necessarily meet all the security function requirements of a ZIP, but they can have a role in network zoning.

Cloud resources are deployed within these specific zones. In a traditional network environment, it would be expected to find a ZIP at the boundary of the zone. Within a cloud environment, a ZIP can be situated at the boundary of a zone, or it can be within a zone associated with specific cloud resource network interfaces, such as a virtual machine (VM) or host.

3.1.1 Virtualization

A common way to isolate web-facing applications is through virtualization. Desktop virtualization is a software-based technology used to create software versions of IT systems and services that are traditionally implemented in separate physical hardware. These software versions, or virtual instances, can dramatically increase efficiency and decrease costs. You can use hardware to its full capacity by distributing its capabilities among many different services.

Desktop virtualization separates the logical desktop from the physical device. The user interacts with the host computer by using another desktop or mobile device that is connected to your organization's network. With regards to applications, you can use virtual desktops to have centralized control over which applications user can access on their workstations.

Using virtualization technology, you can encapsulate an application so that it's separate from other programs or from the operating system (OS) on which it's running. Although the application still executes and runs as intended, it's not installed on the host.

3.1.1.1 Virtual machine (VM)

With virtualization, you can run your applications on fewer physical servers. Applications and software run virtually on a simulated computer system called a VM. A VM is the emulated equivalent of a computer system that runs on top of another system. By using a VM, you can run applications in isolated environments. You could also use a container, which is an isolated process but isn't a full, independent machine. When using a container, applications can run in isolated user spaces like a VM. However, unlike VMs, each container shares the same underlying host OS and sits on top of a physical server.

The VM has all the features of a computer server, without needing the physical hardware attached and is supported by a hypervisor.

3.1.1.2 Hypervisor

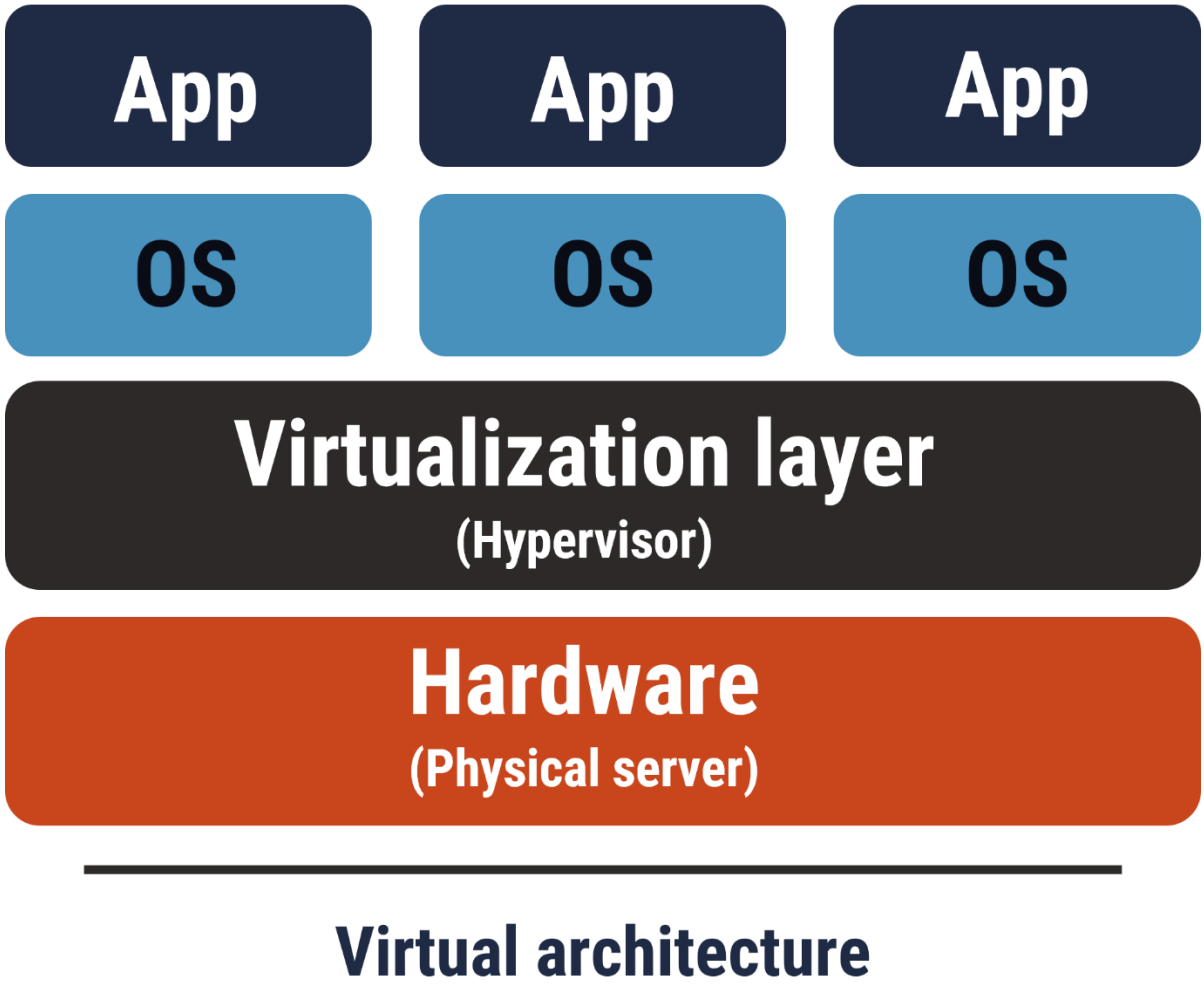
The hypervisor is software that delivers the necessary computing resources, like storage or memory, to multiple VMs, enabling them to run virtually.

There are two types of hypervisors: bare-metal and hosted. A **bare metal hypervisor** runs directly on physical hardware, while a **hosted hypervisor** runs as an application on a host OS.

3.1.1.3 Hardware servers

A single hardware server may support multiple VMs. Without virtualization, idle applications have resources such as processing power or RAM, storage that are unused. With virtualization, hardware servers can be used at full capacity to offer the hypervisor all the resources necessary to support the VMs.

Figure 3: Virtualized environment



3.2 Apply the principle of least privilege (AC-6)

Your organization should implement the principle of least privilege. Essentially this means you grant a user only the set of privileges that are required to perform authorized tasks. This principle limits the damage that can result from accidental, incorrect, or unauthorized use of an application.

When deploying an application, you should ensure that users only have the level of access that is needed for the application to function. 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 should also use the principle of least privilege when allowing remote access to your devices.

In cloud-native environments, a strong security posture is linked to robust identity and access management (IAM). The cloud management zone (MZ) IAM service requires organizations to implement role-based access control (RBAC) to control permissions for users and resources. RBAC should be structured to enforce least privileged access. The cloud MZ is a dedicated and isolated administration network available to network administrators for configuring and monitoring network infrastructures

Using separate processing domains enables you to allocate user privileges more specifically. 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.

Summary

One of our top 10 recommended IT security actions is to isolate web-facing applications. To do this effectively, we recommend using virtualization to create a separate environment on which applications can run and implementing least privilege for all application users. The guidance in this document is based on security controls AC-6 and SC-32, which are detailed in Annex A of this document.

Isolating web-facing applications prevents malware from spreading to other hosts and systems. However, isolating your organization's web-facing applications is just one aspect of improving cyber security. To best protect your organization again cyber threats, you should review and implement all the actions recommended in ITSM.10.189 Top 10 IT Security Actions to Protect Internet Connected Networks and Information [1].

For more information on application security, see ITSM.10.095 Top 10 IT Security Actions: No. 10 Implement Application Allow Lists [4] which provides guidance on creating a list of applications that are authorized to run on your organizations systems. An application allow list is an effective way to prevent unauthorized and malicious programs from executing on organizational systems. As an additional layer of security, your organization should patch and update your OS and applications frequently. For more information on patching, see ITSM.10.096 Top 10 IT Security Actions: No. 2 Patch Operating Systems and Applications [5] which includes best practices for managing updates and patches for your OS and applications.

4 Supporting content

4.1 List of abbreviations

Term	Definition
AC	Access control (security control family code)
CCCS	Canadian Centre for Cyber Security
IAM	Identity and access management
IT	Information technology
MZ	Management zone
OS	Operating system
RBAC	Role-based access control
SC	System and communications protection (security control family code)
SQL	Structured language query
VM	Virtual machine
XSS	Cross-site scripting
ZIP	Zone interface point

4.2 Glossary

Term	Definition
Application allow list	A list of specific applications and application components (e.g., executable programs, software libraries, configuration files) that are authorized to install and execute on organizational systems.
Availability	A value that is assigned to information assets, software, and hardware (infrastructure and its components). Data with the highest possible availability rating must always be accessible. Implied in its definition is that availability includes the protection of assets from unauthorized access and compromise.
Confidentiality	A value that is assigned to a set of information to indicate its sensitivity level and any access restrictions that prevent unauthorized people from accessing it.
Containerization	The complete isolation of one technology from another.
Cross-site scripting	An attack method in which a threat actor takes advantage of security flaws and injects malicious script into a benign and trusted web application.
Cyber attack	The use of electronic means to interrupt, manipulate, destroy, or gain unauthorized access to a computer system, network, or device.
Denial of service	Any activity that makes a service unavailable for use by legitimate users, or that delays system operations and functions.
Integrity	A value that is assigned to information to indicate how sensitive it's to data loss. Implied in its definition is that integrity includes protecting information from being modified or deleted

Term	Definition
	unintentionally or when it's not supposed to be. Integrity helps determine that information is what it claims to be. Integrity also applied to business processes, software application logic, hardware, and personnel.
IT asset	The components of an information system, including business applications, data, hardware, and software.
Management security control	A class of security controls that focus on the management of IT security and IT security risks.
Operational security control	A class of security controls primarily implemented and executed by people and typically supported by technology (e.g., supporting software).
Risk	The likelihood and the impact of a threat using a vulnerability to access an asset.
Sandbox	A virtual space in which new or untested software can be run securely and its behaviour can be observed before it's allowed onto a domain or system.
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.
SQL injection	An attack method in which a threat actor takes advantage of security design flaws in web forms to inject malicious code or code used for malicious purposes.
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.
Virtualization	Technology that you can use to create simulated environments or virtual resources (e.g. server, desktop, operating system, storage, network).
Virtual machine	A computer with an operating system that can run applications but that does not physically exist. It's an emulated equivalent of a computer system.
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.
Web-facing application	Any program that can be accessed over a network connection and uses web technology and browsers to perform tasks over the Internet (e.g., email, word processors, file conversion, e-commerce, calendars).

4.3 References

Number	Reference
1	Canadian Centre for Cyber Security. ITSM.10.189 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. December 2014.

Number	Reference
3	Open Web Application Security Project. Top 10 Web Application Security Risks. March 2021.
4	Canadian Centre for Cyber Security. ITSM.10.095 Top 10 IT Security Actions: No. 10 Implement Application Allow Lists. August 2022.
5	Canadian Centre for Cyber Security. ITSM.10.096 Top 10 IT Security Actions: No. 2 Patching Operating Systems and Applications. August 2022.

Annex A ITSG-33 security control catalogue

A.1 Technical security controls: Access control

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

Table 2: ITSG-33 technical security control: AC-6 least privilege

Number	Control	Requirement	Control enhancements	Related ITSG-33 controls
AC-6	Least privilege	(A) The organization applies the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) that are 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

A.2 Technical security control: System and communications protection

Table 3 describes control **SC-32 Information System Partitioning**, as defined in Annex 3A of ITSG-33 [2].

Table 3: ITSG-33 technical security control: SC-32 information system partitioning

Number	Control	Requirement	Control enhancements	Related ITSG-33 controls
SC-32	Information system partitioning	(A) The organization partitions the information system into [organization-defined information system components] residing in separate physical domains or environments based on [organization-defined circumstances for physical separation of components*]*.	None.	AC-4 SA-8 SC-3 SC-7