Communications Security Establishment | Centre de la sécurité des télécommunications

CANADIAN CENTRE FOR CYBER SECURITY

Top 10 IT security actions:

No. 5 segment and separate information

MANAGEMENT

Canada

Foreword

This document is an UNCLASSIFIED publication issued under the authority of the Head of the Canadian Centre for Cyber Security (Cyber Centre). 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 November xx, xxxx.

Revision history

Revision	Amendments	Date
1	First release of publication.	Month XX, 20XX

Overview

This document is part of a suite of documents that focuses on the top 10 IT security actions recommended in Top 10 IT security actions to protect Internet connected networks and information (ITSM.10.089) [1][1]. Part of the top 10 IT security actions is to segment and separate information.

All organizations should have an inventory of their essential business information. These information stores should be classified and categorized taking into consideration any protection requirements based on the sensitivity or privacy impact of information. Networks should be zoned by segmenting and grouping infrastructure services that have the same information protection requirements or that must adhere to the same communication security policies. This logical design approach is used to control and restrict access and data communication flows. Further, organizations should monitor and enforce controls to maintain zone protection and integrity. For additional guidance, consult the Cyber Centre's Baseline security requirements for network security zones (ITSP.80.022) [2] and ITSG-38 Network security zoning: Design considerations for placement of services within zones [3].

While implementing all 10 of the recommended IT 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

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

Table of contents

List of figures

List of tables

List of annexes

1 Introduction

This document provides guidance on how you can segment your networks into various security zones. Network segmentation separates similar information technology (IT) assets, like hardware, software, and data, into logical groupings that have the same security policies and security requirements. Segmentation reduces your organization's exposure to threats that could exploit vulnerabilities and compromise your networks, systems, and IT assets. This guidance expands on the advice in Top 10 IT security actions to protect Internet connected networks and information (ITSM.10.089) [1] and the security controls listed in Annex - 3A Security control catalogue of ITSG-33 IT security risk management: A lifecycle approach [4].

1.1 Top 10 IT security actions

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

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

When determining your security needs, you should also consider whether your organization will use an on-premise (on-prem) model or outsource to a cloud service provider (CSP) or a managed service provider (MSP). If you decide to work with a CSP or MSP, you should assess the threats, vulnerabilities, shared responsibilities, and cloud platform capabilities so that you can implement appropriate security controls. The ways in which you follow the top 10 may differ depending on the types of services you are using. For example, the roles and responsibilities of your organization and your CSP or MSP will vary depending on the services they are providing, your service model, and your deployment model. However, even when using cloud or managed services, your organization is still legally responsible and accountable for securing its data. For more information on security and cloud or managed services, see Cloud security risk management (ITSM.50.062) [5] and Cyber security considerations for consumers of managed services (ITSM.50.030) [6].

Figure 1: Top 10 IT security actions – No. 5 segment and separate information

1.2 IT security risk management process

Our top 10 security actions are based on the security controls listed in Annex 3A of ITSG-33 [4]. ITSG-33 [4] is a risk management framework which describes the roles, responsibilities, and activities that help organizations manage their IT security risks. It includes a catalogue of security controls like 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:

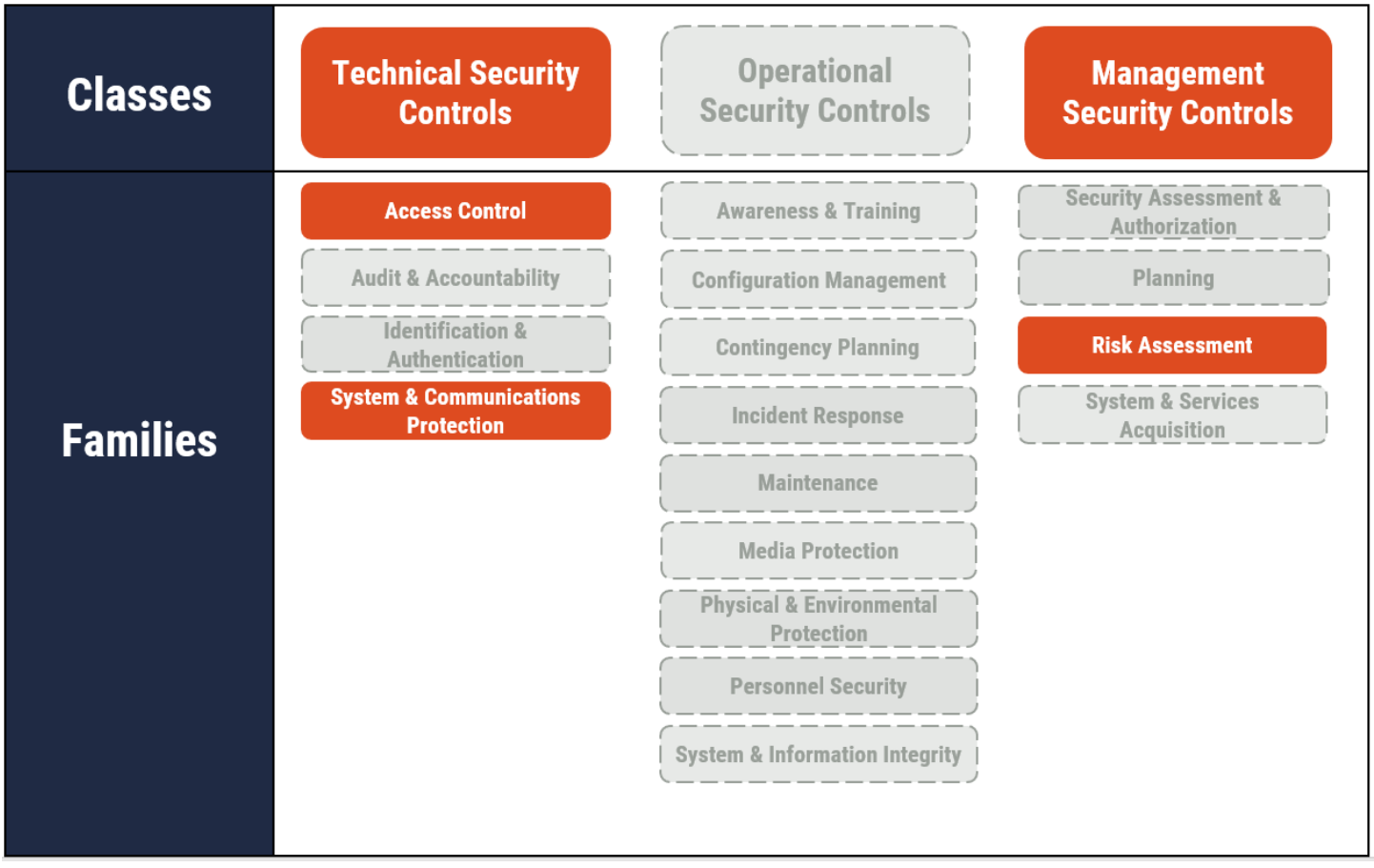
- **Technical security controls:** Security controls that are implemented and executed by information systems primarily through security mechanisms contained in hardware, software, and firmware components.
- **Operational security controls:** Information system security controls that are primarily implemented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

As illustrated in Figure 2, the guidance in this document addresses technical security controls that fall under the access control (AC) and systems and communications protection (SC) families. It also addresses management security controls that fall under the risk assessment (RA) family. This document includes actions that help satisfy the following security controls:

- **AC-4 information flow enforcement**
- **SC-2 application partitioning**
- **SC-3 security function isolation**
- **SC-7 boundary protection**
- **SC-32 information system partitioning**
- **RA-2 security categorization**

See Annex A of this document for more information on controls AC-4, SC-2, SC-3, SC-7, SC-32, and RA-2.

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



You can use the security controls discussed in this document and in Annex 3A of ITSG-33 [4] as a foundation when determining how to manage your organization's cyber security risks and protect its networks, systems, and IT assets. However, keep in mind that implementing these controls is only one part of the IT security risk management process.

ITSG-33 [4] describes a process based on two levels of risk management activities: departmental-level activities and information system-level activities. These two levels of activities will help your organization identify its security needs for both the entire organization and its information systems. Once you understand your security needs at each level, you can identify which security controls your organization needs to implement and maintain based on your accepted level of risk.

2 Controls supporting network segmentation

2.1 Information flow enforcement

The guidance in this section is based on security control **AC-4 information flow enforcement.**

When creating security zones within your environment, in addition to defining who has access to the data within them, it is also necessary to define what information is permitted to travel between them, in addition to defining who has access to the data within them. Enforcing the flow of information both between and within security zones allows your organization to control data flow across your network. This will ensure sensitive or classified information cannot travel across your systems unless otherwise defined in your segmentation rules. Flow control restrictions can include blocking external traffic that claims to be from within your organization or restricting web requests to the Internet that are not from your organization's internal web proxy server. This concept can be applied for both traditional network zoning, which commonly leverages routable Internet protocol (IP) subnets, and for software-defined networks (SDN) or cloud segmentation that may instead segregate by dynamic policy or asset tagging.

Your organization should develop information flow control policies that clearly define the boundaries of where and how information can flow within and between your information systems. These policies should be clearly written, readily available, and frequently reviewed to ensure your information remains protected. Some policies or security control rules you may want to implement could include prohibiting information transfers between interconnected systems or employing hardware that works to enforce one-way information flows within your network.

Enforcement mechanisms should be deployed to control the flow of information between designated sources and destinations, like your networks, devices, and users, within and between your systems. This enforcement can occur via your organization's boundary protection controls and devices, such as your routers, firewalls, and protected gateways. These controls and devices have been configured to restrict information system services and provide filtering capabilities, like packet filtering or message filtering, based on predefined rules or settings.

2.2 Security categorization

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 organization's information to identity its value, determine its classification, and categorize it into groups, based on its level of sensitivity.

2.2.1 Identify its value

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, like sales information or emergency response plans
- **Sensitive information:** Information that needs to be kept confidential or only accessed by certain users, like financial and personal information or intellectual property
- **Records and evidence**: Information that needs to be protected from unauthorized modification, like contracts and receipts

For more information on determining the value of information systems and assets, see Protecting high value information: Tips for small and medium organizations (ITSAP.40.001) [7] and section 2.3 of our Baseline cyber security controls for small and medium organizations [8].

2.2.2 Classify and categorize

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 and protect it against unauthorized access and distribution, as well as improper retention and disposition.

Categorizing your enterprise information has several purposes, including:

- reflecting the value that your organization has assigned to the information
- representing your organization's risk tolerance
- determining 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 predetermined risk tolerance.

2.3 Application partitioning

The guidance in this section is based on the security control **SC-2 application partitioning.**

The separation of user functionality from information system management functionality is critical. Information system management functionality includes, for example, functions necessary to administer databases, network components, workstations, or servers, and typically requires privileged user access. Your organization should set up your information systems to separate user functionality and privileges from IT systems administrative functions or privileges.

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
- 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).

You should disallow privileged users from having one account with both normal user access to networks, such as the Internet and email services, and administrative privileges. Whether your organization uses a cloud, on-prem, or hybrid environment, we strongly recommend that you create separate administrative accounts with separate credentials 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. You should develop a policy or directive that ensures all administrative tasks are performed on dedicated administrative computers that cannot access the Internet or email services. For remote access, Annex 3A of ITSG-33 [4] 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 is configured with a virtual private network (VPN) or allow lists, and multi-factor authentication (MFA) to access the cloud tenancy.

For more information on administrative accounts and permissions, see Top 10 IT security actions: No. 3 managing and controlling administrative privileges (ITSM.10.094) [9].

3 Network segmentation: An introduction

Network segmentation is an IT security approach that divides a network into multiple smaller segments that can enhance both the performance and security of your IT environment. It separates similar IT assets, like hardware, software, and data, into logical groupings that have the same security policies and security requirements. More specifically, network segmentation is a security architectural technique that leverages subnets or other grouping methods to divide a network into smaller, distinct, compartmentalized groups that enables your organization to deliver unique security controls and services.

Whether using subnets, tagging, or other methods the intent is that the group acts as its own separate network within your IT environment. This provides administrators the ability to control the flow of traffic between defined groups to meet your organization's policies and applied security controls. The unique security controls applied to the flow between groups are defined within a zone interface point (ZIP).

In a traditional security zone architecture, a ZIP is a system that monitors and controls the flow of information between two security zones. The dividing lines 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 two zones by creating a distinct communication path.

While the concept of a ZIP still exists within software defined networks (SDN) or cloud networks, it is typically broken up as a stack of one or more virtual appliances that combined, provide monitoring and control the flow of information between asset groups. While traditional security zone architecture provided a clear boundary between zones where the ZIP resided, in SDN or Cloud this is accomplished by routing traffic virtually through the security stack.

The guidance in this section is based on security control **SC-3 security function isolation, SC-7 boundary protection** and **SC-32 information system partitioning.**

SC-3 security function isolation states that the information system must isolate security functions from non-security functions, by means of an isolation boundary. Isolation enhances access control and protects the integrity of your organization's hardware, software, and firmware. Your organization should ensure your network is set up in such a way that security-related functions are isolated from non-security functions. To enhance your organization's ability to setup your network to isolate security-related functions from non-security functions, you should:

- implement the principle of least privilege which provides users the minimal level of access and permissions required to perform their assigned tasks
- apply access control mechanisms
- implement dual authorization mechanisms for administrative and root tasks
- enforce MFA wherever possible (particularly for administrative accounts)
- dedicate workstations for privileged users to perform administrative duties
- deploy collaborative administration where multiple administrators are required to confirm administrative operations
- use hardware separation mechanisms, such as configuring the hierarchical protection domains (protection rings) of your operating systems
- implement virtualization technologies to isolate processes related to security functions
- configure separate administrator accounts from user accounts with the appropriate level of access and privileges

SC-7 boundary protection states the information system must do the following actions:

- Monitor and control communications at the external boundary of the system and at key internal boundaries within the system
- Implement sub-networks for publicly accessible system components that are physically and logically separated from internal organizational networks
- Connect to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture

SC-32 information system partitioning states the organization must partition the information system into organizationally defined system components that reside in separate physical domains or environments based on organizationally defined circumstances for physical separation of the components. Security categorization can assist in identifying the components that need to be partitioned and can be managed by an interface that restricts or prohibits network access and information flow amongst partitioned components. Within your segmented network, we recommend that web-facing applications be restricted from accessing the network or communicating with other information systems outside of the subnet or zone they reside in. This will enhance the protection of your network, as applications that become infected with malware or exploited cannot spread to other parts of your environment and infect other hosts or systems.

4 Network segmentation: Practical application

Segmenting your networks into various security zones is part of a defence-in-depth approach to cyber security. It limits access to connected systems, applications, devices, and data. Segmentation restricts communication between networks, thus isolating sensitive data and restricting access from unauthorized users. Network security zones can support a range of security solutions for your organization's business needs. These security zones also provide a common network infrastructure to support electronic service delivery, interconnectivity, and interoperability. If your organization shares a common infrastructure for online service delivery or other purposes, you must conform to all the security standards established for that infrastructure.

Network segmentation reduces the attack surface, as it prevents widespread compromise of your organization's network. If a host on one network is compromised, the hosts on the other network segments will not be impacted by the compromise, as they are unreachable beyond the boundaries of the segmented network that the compromised host resides in.

4.1 Segmentation considerations

Network segmentation requires planning and standard best practices to be successful. The following list provides some industry-accepted best practices you should implement prior to segmenting your networks into security zones.

- Conduct an inventory of your data and assets.
- Classify your data and assets as high, medium, or low value.
- Draft and implement security policies to be applied to each type of data and asset that requires protection. The level of risk assigned to the data or assets will dictate the level of security required to protect them, as well as the details of the security policy assigned.
- Follow the principle of least privilege, meaning your users are given only the set of access privileges that are essential for them to perform authorized tasks. This principle limits the damage that can result from the accidental, incorrect, or unauthorized use of an information system.
- Determine who needs to access your data and develop a rule-based access (RuBAC) or role-based access (RBAC) rights model.
- Limit third party access to your network to avoid creating additional entry points that can be exploited by threat actors. Identify the data flow for each of your applications and implement application allow lists to deny unapproved applications from executing on your systems. For more information on application allow lists, see the Cyber Centre's Top 10 security actions – No.10 implement application allow lists (ITSM.10.095) [10].
- Monitor and audit your network on a continuous basis to identify anomalies in traffic patterns. For more information on auditing, monitoring, and logging, see the Cyber Centre's Network security logging and monitoring (ITSAP.00.085) [11] and Network security auditing (ITSAP.80.086) [12].
- Implement sensors within each of your network segments to alert of potential intrusions. The logs from these sensors should be maintained and backed up to secure, offline storage.

Network segmentation can be implemented in a variety of IT environments. Whether your organization uses an on-prem, cloud, or hybrid IT environment, segmenting your networks into security zones will enhance your data security and reduce your risk of unauthorized access or compromised data.

Your organization's implementation of network security zones should align with your current IT security risk management activities, such as defining organizational IT security needs and security controls, deploying security controls, and monitoring and assessing the performance of security controls. Your implementation should also align with your information system-level activities to ensure the solution is functional.

The following subsections provide information and best practices on implementing network segmentation in an on-prem, cloud, or hybrid IT environment. Guidance for organizations with operational technology (OT) is also provided.

Note: For hybrid environments, the guidance provided in the on-prem and cloud sections can be leveraged in tandem to address segmentation best practices.

4.2 Segmentation on-prem

On-prem environments, where IT infrastructure and security elements are managed in-house, have traditionally leveraged perimeter-based segmentation. In this model, subnets and external networks only connect to one another through managed interfaces, such as gateways, routers, or firewalls. For example, a firewall can be implemented at an Internet gateway to protect internal networks. Firewalls can also be used to define and protect a subnet hosting specific applications.

Subnets that physically or logically separate external untrusted networks from internal networks are referred to as demilitarized zones (DMZs). DMZs are typically protected with firewalls and shield internal networks from external threat actors seeking to gain unauthorized access. DMZ managed interfaces often restrict external web traffic to designated web servers and prohibit external traffic that appears to be spoofing internal addresses.

4.2.1 Virtual local area network (VLAN)

A VLAN is a virtualized connection that joins devices and nodes across your network. They are used to assist in the division of your network into subnets and the isolation of traffic from other established VLANs. Your organization can use them to assist in limiting traffic from other areas in your environment and enable subnets to be connected across your network, despite their physical location.

You can improve your network performance by segmenting your network into subnets and VLANs, as they reduce the volume of broadcast traffic being sent or received by your network.

VLANs are often used in combination with access control lists (ACLs) to enhance the filtering of traffic on your network. Your organization can implement ACLs on your routers and switches to further enhance your IT security posture. The ACLs will better isolate your devices and systems, which can enhance your organization's ability to prevent threat actors from deploying and spreading malware across your network.

Note: VLANs are used for IP management and while they can be useful in limiting broadcast traffic and allow for asset management on the network, they are not a security solution for network segregation.

4.2.2 Firewalls

Firewalls, or devices with firewall capabilities, are essential to network segmentation. A firewall is a security barrier placed between two networks that controls the amount and types of traffic that may pass between them. This protects local system resources from being accessed from the outside. They can be physically in the path of the network traffic (inline) or be encountered by this traffic logically, because of the routing rules in effect on the network. A firewall assesses every network packet to ensure it complies with rules established in policy and enforced by the administrator before allowing it through.

Firewalls can also include additional functions, such as anti-malware, intrusion detection and prevention capabilities, or they can serve as remote connection VPN termination points. All traffic going through your firewall should be logged in detail, as these logs can provide valuable information about normal traffic patterns and help spot irregular or malicious traffic. The logs can be used to establish a baseline for normal traffic patterns for your organization and will assist you in spotting anomalies in those patterns. These anomalies can be indicative of malicious activity. Your organization should also backup your logs to a read-only location, such as a different email or offline storage, to protect them from being compromised by a threat actor.

Firewalls can be both physical, like a hardware device, or virtual, like a cloud-based or virtual firewall running in a virtual environment. Depending on the architecture and the criticality of systems, it might be advisable to use multiple firewalls to secure critical networks even further. For example, you can have one firewall act as a gatekeeper to another firewall in an on-prem or hybrid environment. Some organizations also opt for using different vendors when using multiple firewalls so that if one manufacturer reports a flaw or security vulnerability, the other might not have the same vulnerabilities.

To move beyond traditional firewall capabilities, your organization could deploy next-generation firewalls. These firewalls provide enhanced functionality, such as content filtering at a higher layer in the Open Systems Interconnection (OSI) model.

4.2.3 Software-defined network (SDN)

SDN is a networking approach that results in the virtualization of networks. With SDN, the physical network infrastructure is abstracted to a fabric layer, and all traffic flow is controlled by a central controller or controllers. SDN can be adapted to your existing architecture and can assist in virtualizing your networks. It uses software-based programs or application programming interfaces (APIs) to communicate with your organization's infrastructure and assist in directing traffic within your segmented network. Being software-based, SDN is more flexible than traditional networking and allows administrators to manage and control several components from a single interface. The need to secure this interface is crucial for your organization, as it could be a single point of failure if it were compromised by a threat actor.

Virtualization is technology that your organization can use to create simulated environments or virtual resources, like your servers, desktop, operating system, storage, or networking components. It separates the logical desktop from the physical desktop. A user then interacts with the logical (virtual) desktop through a device connected to your organization's network. This device can be a workstation or mobile device and may have its own separate desktop. You can use virtual desktops to centrally control which applications users can access on their workstations.

While virtualized devices can still be managed in a traditional IT way, SDN relies on devices being physically connected to an underlay and central management.

4.2.4 Micro-segmentation

With traditional network segmentation approaches, the focus is on network traffic from a client to your organization's server. When data comes from outside your organization's network, security controls filter it to the appropriate subnet. The limitation to this is that traditional segmentation cannot monitor the traffic within your network security zones themselves. To further segment and monitor traffic within your network, you may want to implement micro-segmentation.

Micro-segmentation works to further segment by applying security controls and protocols to the traffic within your network security zones. Micro-segmentation allows your organization to isolate specific individual applications, which means if the application itself is ever compromised, the threat cannot spread to other areas within your network.

Micro-segmentation logically divides the data centres and cloud environments into distinct security segments down to individual workload level. It relies heavily on the use of managed policy enforcement points throughout the network to dynamically control the communication between components based on policy. This is done to protect sensitive data and services from both internal and external threats. It provides layered security and allows for restricted access to assets on a granular level. This ensures that, even if a threat actor does enter the network, the amount of damage they can cause is limited.

Unlike traditional network segmentation, which leverages ZIPs to govern access to network security zones, micro-segmentation can restrict user access to an individual device or a grouping of devices. It can also restrict access to endpoints and applications, despite the VLAN they have been assigned. Another main difference between traditional segmentation and micro-segmentation is the traffic flow direction. Traditional segmentation focuses on north-south traffic, which flows further into or out of the network. Micro-segmentation seeks to control east-west traffic, which flows within a network security zone, or between similar security zones.

There are other differences in the way micro-segmentation functions when compared to traditional segmentation. For example:

- it is applied in smaller subsets of components, often made up of single devices
- it works best with virtual networks
- it follows more granular policies
- it is implemented at the software-level

4.2.5 Challenges of network segmentation

Leveraging network segmentation for security purposes comes with challenges. Often, segmentation needs do not match the network architecture. Re-architecting the networks or reconfiguring VLANs and subnets to meet segmentation requirements is a difficult and time-consuming endeavour.

Architecting segmented networks in an already established IT environment can be time consuming and challenging. If your organization lacks in-house expertise, you may need to outsource the assistance of an IT security professional who can re-architect your environment. These services can be costly and out of reach for many organizations with limited resources.

While segmenting your network can ultimately improve performance, it can be impacted negatively by over-segmenting. Increasing the granularity of segmentation of your networks can potentially create a bottleneck in your network and slow performance.

Another challenge with traditional or perimeter-based segmentation is the established trust framework. With perimeter segmentation, the components within the perimeter of the network are trusted and anything outside of that perimeter is not. While this is an effective security approach to some degree, changes in technology and IT environments, as well as the ability for threat actors to refine their attack methodology, has created a need for more robust trust rules to be applied to networks.

One solution to this challenge is applying the principle of zero trust (ZT) to your environment. At its core, the ZT principle ensures that inherent trust is never granted by default to any subject, whether internal or external to your environment. This principle can be applied to your organization's architecture by implementing zero trust architecture (ZTA).

Lastly, the preventative measures mentioned in earlier sections of this publication, such as firewalls, ACLs, VLANs, DMZs, and SDNs, can all present their own vulnerabilities. Whether your equipment is physical or virtual, threat actors can attempt to gain internal access, bypass firewalls, and VLAN hop, amongst other common attack methods. To mitigate the risk associated with these preventative measures, your organization should review, update, and reconfigure them on a regular basis.

4.2.6 Zero trust architecture (ZTA)

The primary goal of ZT is to prevent or limit the reliance on implicit trust policies when processing traffic flows. It also prevents lateral movement within your IT environment. ZTA is not focused on eliminating the legacy boundary defence your organization may have in place.

ZTA ensures that every interaction initiated between a user and a resource is strongly authenticated and authorized. Access control and permissions are implemented at the most granular level possible, and these access decisions are based on dynamic evaluation of the trust context for each access request.

With ZT the communication between users, systems, and devices is continuously authenticated, authorized, and validated. ZT is founded on policy-based access controls (PBAC), such as RBAC and attribute-based access control (ABAC). A ZTA enforces access policies based on context such as the user's role, the time of day, geolocation, the device, and the data the user is requesting. The level of access that is granted is dynamically adjusted based on the level of trust established with the subject. In short, the more trust that an information system can develop in a subject, the more access that subject can be granted.

For more information on ZTA, see A zero trust approach to security architecture (ITSM.10.008) [13].

4.3 Segmentation in the cloud

The principles of zoning still apply if your organization is using cloud or managed services. If using a shared cloud deployment model, for example, you should ensure that your data is separated from other tenants' data.

As with on-prem segmentation, segmentation in the cloud still employs ZIPs 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 within a zone associated with specific cloud resource network interfaces, such as a virtual machine (VM) or host.

In a cloud environment, networking has evolved to using SDN. Compared with traditional networking, SDN has different characteristics and capabilities that need to be taken into consideration in the use of segmentation of network security zones in a cloud environment.

Some of the key differences with traditional networking are:

1. decoupling of the control plane, which specifies how traffic is routed within the SDN, from the device data plane, which physically handles the traffic as dictated by the control plane
2. centralized single point of configuration provisioning and management
3. central control point for regulating granular security and policy information

It is important to understand that while the CSP provides management and control plane access to its SDN, that access is exposed through their resource abstraction and control layer, a software as a service-like (SaaS-like) model. The CSP does not provide direct access to its SDN nor its implementation, whether that is in software or hardware. It is part of the CSP fabric.

Both on-prem and cloud environments share the same foundational principles of controlling, restricting access and data communication flows to certain components and users. They both establish network perimeters and associated boundary controls through the following functions:

- Defining the entities that populate zones
- Identifying discrete zone entry and exit points
- Filtering network traffic at entry and exit points
- Monitoring the state of the network
- Authenticating the identity of network devices and users
- Monitoring network traffic at the entry and exit points

For more guidance on a defence-in-depth approach, and segmentation, for cloud, see Guidance on defence-in-depth for cloud-based services (ITSP.50.104) [14] and Cloud network security zones (ITSP.80.023) [15].

4.3.1 Cloud zoning responsibilities

For SaaS offerings, the CSP is responsible for network zoning of the cloud environment. For platform as a service (PaaS) offerings, in which the CSP is typically hosting multiple tenants, platforms will most likely be subject to the CSP's network zoning practices. Your organization has the responsibility to ensure that SaaS or PaaS applications comply with your organizational security policy especially on network zoning. The security requirements that a business application must meet are derived from the organization security policy or the risk management framework. ITSG-33 [4] can be used as part of the risk management framework to determine the security controls your organization should implement. Threat modeling, including identifying specific threats, should be part of your organization's risk management framework.

Your organization should limit third-party service provider access to your network. Remote access points can increase the number of entry points into your network. These entry points can be exploited by threat actors and used as vectors to conduct malicious activities, such as deploying malware onto your network.

4.4 Segmentation for operational technology (OT)

Many of the network segmentation best practices and recommendations from Section 2.0 are applicable to OT environments. However, there are specific items that critical infrastructure organizations should establish to better protect their OT and industrial control systems (ICS). Separating your OT from your IT is paramount in an effective cyber security strategy. This separation will ensure that ICS function as they need to, without being connected to networks that could potentially become infected by malware.

Firewalls are an effective security tool, and it is strongly recommended that OT environments have them implemented. It is possible to take a layered approach with firewalls in an OT environment. For example, a single OT firewall could secure connections out to the IT network and feeds to external service providers or vendors, while also isolating all DMZ traffic. At the same time, internal firewalls can have highly granular policies for controlling flows between critical networks and devices, such as supervisory control and data acquisition (SCADA) systems. In general, a “deny all” approach is recommended for all OT connectivity, which allows your organization to implement firewalls to limit system communication with other systems, which will disallow any ad-hoc connectivity or lateral movement. This is another way in which your organization can layer your defensive posture and better protect your network, systems, and data.

5 Summary

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.

One of our top 10 recommended IT security actions is to segment and separate information. The guidance included in this document is based on several of the security controls detailed in Annex 3A of ITSG-33 [4]. This document is not comprehensive or all-encompassing. To best segment and separate your information, you should review the guidance in this publication and apply the security controls discussed. You should also review the other top 10 recommended IT security actions in ITSM.10.089 [1].

6 Supporting content

6.1 List of abbreviations

Term	Definition
ABAC	Attribute-based access control
ACL	Access control list
API	Application program interface
CI	Critical Infrastructure
CSE	Communications Security Establishment
CSP	Cloud service provider
DMZ	Demilitarized zone
GC	Government of Canada
ICS	Industrial control systems
IT	Information technology
ITS	Information technology security
MFA	Multi-factor authentication
MSP	Managed service provider
OSI	Open systems interconnection
OT	Operational technology
RBAC	Role-based access control
RuBAC	Rule-based access control
SDN	Software-defined network
VPN	Virtual private network
ZIP	Zone Interface Point
ZT	Zero trust
ZTA	Zero trust architecture

6.2 Glossary

Term	Definition
Attack surface	The set of points on the boundary of a system, a system element, or an environment where an attacker can try to enter, cause an effect on, or extract data from, that system, system element, or environment.
Authentication	The process of verifying an identity claimed by or for a system entity [14].
Authorization	Access privileges granted to a user, program, or process [15].

Term	Definition
Boundary	A portion of the perimeter of a zone or network that is the point of connection between two zones or networks.
Firewall	A security barrier placed between two networks that controls the amount and kinds of traffic that may pass between the two. This protects local system resources from being accessed from the outside.
Least privilege	The principle of giving an individual only the set of privileges that are essential to performing authorized tasks. This principle limits the damage that can result from the accidental, incorrect, or unauthorized use of an information system.
Multi-factor authentication	A tactic that can add an additional layer of security to your devices and account. Multi-factor authentication requires additional verification (like a PIN or fingerprint) to access your devices or accounts. Two-factor authentication is a type of multi-factor authentication.
Need to know	Primarily associated with organizations that assign clearance levels to all users and classification levels to all assets; restricts users with the same clearance level from sharing information unless they are working on the same effort. Entails compartmentalization. (ISC² Glossary).
Network security zone	A networking environment with a well-defined boundary, a Network Security Zone Authority, and a standard level of weakness to network threats. Types of zones are distinguished by security requirements for interfaces, traffic control, data protection, host configuration control, and network configuration control.
Operational technology	Programmable systems or devices that interact with the physical environment (or manage devices that interact with the physical environment). These systems/devices detect or cause a direct change through the monitoring and/or control of devices, processes, and events.
Perimeter	The boundary between two network security zones through which traffic is routed.
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 that can include security products, security policies, security practices, and security procedures.
Security perimeter	The boundary of the domain in which a security policy or security architecture applies (i.e. the boundary of the space in which security services protect system resources) [14].
Subnet	Short for subnetwork. A portion of a network, which may be a physically independent network segment, that shares a network address with other portions of the network and is distinguished by a subnet number. A subnet is to a network what a network is to an internetwork.
Virtualization	A software-based technology used to create software versions of IT systems and services that are traditionally implemented in separate physical hardware. The simulation of the software and hardware upon which other software runs.
Virtual private network	A private communications network usually used within a company, or by several different companies or organizations to communicate over a wider network. VPN communications are typically encrypted or encoded to protect the traffic from other users on the public network carrying the VPN.
Zone interface point	An interface between two network security zones through which traffic may be routed.

6.3 References

Number	Reference
1	Canadian Centre for Cyber Security. Top 10 IT Security Actions for Internet Connected Networks and Information (ITSM.10.089). September 2021.
2	Canadian Centre for Cyber Security. Baseline Security Requirements for Network Security Zones (ITSP.80.022). January 2021.
3	Canadian Centre for Cyber Security. ITSG-38 Network Security Zoning – Design Considerations for Placement of Services within Zones. May 2009.
4	Canadian Centre for Cyber Security. ITSG-33 IT Security Risk Management: A Lifecycle Approach. November 2012.
5	Canadian Centre for Cyber Security. Cloud Security Risk Management (ITSM.50.062). March 2019.
6	Canadian Centre for Cyber Security. Cyber Security Considerations for Consumers of Managed Services (ITSM.50.030). October 2020.
7	Canadian Centre for Cyber Security. Protecting High-Value Information: Tips for Small and Medium Organizations (ITSAP.40.001). April 2019.
8	Canadian Centre for Cyber Security. Baseline Cyber Security Controls for Small and Medium Organizations. February 2020.
9	Canadian Centre for Cyber Security. Top 10 IT Security Actions: No. 3 Managing and Controlling Administrative Privileges (ITSM.10.094). July 2022.
10	Canadian Centre for Cyber Security. Top 10 Security Actions – No.10 Implement Application Allow Lists (ITSM.10.095). August 2022.
11	Canadian Centre for Cyber Security. Network Security Logging and Monitoring (ITSAP.00.085). December 2022.
12	Canadian Centre for Cyber Security. Network Security Auditing (ITSAP.80.086). December 2022.
13	Canadian Centre for Cyber Security. A Zero Trust Approach to Security Architecture (ITSM.10.008). February 2023 (update link when published)
14	Canadian Centre for Cyber Security. Guidance on Defence-in-Depth for Cloud-Based Services (ITSP.50.104). May 2020.
15	Canadian Centre for Cyber Security. Cloud Network Security Zones (ITSP.80.023). June 2023.

Annex A ITSG-33 security control catalogue

A.1 Technical security controls

A.1.1 Access control

Table 1 lists the applicable access control, as defined in Annex 3A of ITSG-33 [4].

Table 1: ITSG-33 access control security controls: AC-4

Number	Control	Requirement	Control Enhancements	Related ITSG-33 Controls
AC-4	Information flow enforcement	(A) The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems based on [*organization-defined information flow control policies*].	**Object security attributes:** The information system uses [*organization-defined security attributes*] associated with [*organization-defined information, source, and destination objects*] to enforce [*organization-defined information flow control policies*] as a basis for flow control decisions. See related security control AC-16. **Processing domains:** The information system uses protected processing domains to enforce [*organization-defined information flow control policies*] as a basis for flow control decisions. **Dynamic information flow control:** The information system enforces dynamic information flow control based on [*organization-defined policies*]. See related security control SI-4.	AC-3 AC-16 AC-17 AC-19 AC-21 CM-6 CM-7 IA-2 IA-3 IA-4 IA-5 SA-8 SC-2 SC-5 SC-7 SC-18

			Content check encrypted information: The information system prevents encrypted information from bypassing content-checking mechanisms by [*Select (one or more): decrypting the information; blocking the flow of the encrypted information; terminating communications sessions attempting to pass encrypted information; [organization-defined procedure or method]]*. See related security control SI-4. **Embedded data types:** The information system enforces [*organization-defined limitations*] on embedding data types within other data types. **Metadata:** The information system enforces information flow control based on [*organization-defined metadata*]. See related security controls AC-16 and SI-7. **One-way flow mechanisms:** The information system enforces [*organization-defined one-way flows*] using hardware mechanisms. **Security policy filters:** The information system enforces information flow control using [*organization-defined security policy filters*] as a basis for flow control decisions for [*organization-defined information flows*]. **Human reviews:** The information system enforces the use of human reviews for [*organization-defined information flows*] under the following conditions: [*organization-defined conditions*]. **Enable / disable security policy filters:** The information system provides the capability for privileged administrators to enable/disable [*organization-defined security policy filters*] under the following conditions: [*organization-defined conditions*].	SI-3 SI-4 SI-7

			Configuration of security policy filters: The information system provides the capability for privileged administrators to configure [*organization-defined security policy filters*] to support different security policies. **Data type identifiers:** The information system, when transferring information between different security domains, uses [*organization-defined data type identifiers*] to validate data essential for information flow decisions. **Decomposition into policy-relevant subcomponents:** The information system, when transferring information between different security domains, decomposes information into [*organization-defined policy-relevant subcomponents*] for submission to policy enforcement mechanisms. **Security policy filter constraints:** The information system, when transferring information between different security domains, implements [*organization-defined security policy filters*] requiring fully enumerated formats that restrict data structure and content. **Detection of unsanctioned information:** The information system, when transferring information between different security domains, examines the information for the presence of [*organization-defined unsanctioned information*] and prohibits the transfer of such information in accordance with [*organization-defined security policy*]. See related security control SI-3. **Domain authentication:** The information system uniquely identifies and authenticates source and destination points by [*Select (one or more): organization, system, application, individual*] for information transfer. See related security controls IA-2, IA-3, IA-4, IA-5.	

			Security attribute binding: The information system binds security attributes to information [*organization-defined binding techniques*] to facilitate information flow policy enforcement. **Validation of metadata:** The information system, when transferring information between different security domains, applies the same security policy filtering to metadata as it applies to data payloads. **Approved solutions:** The organization uses [*organization-defined solutions in approved configurations*] to control the flow of [*organization-defined information*] across security domains. **Physical / logical separation of information flows:** The information system separates information flows logically or physically using [*organization-defined mechanisms and/or techniques*] to accomplish [*organization-defined required separations by types of information*]. **Access only:** The information system provides access from a single device to computing platforms, applications, or data residing on multiple different security domains, while preventing any information flow between the different security domains.	

A.1.2 Systems and communications protection

Table 2 lists the applicable systems and communication protections, as defined in Annex 3A of ITSG-33 [4].

Table 2: ITSG-33 systems and communications protection: SC-2, SC-3, SC-7, SC-32

Number	Control	Requirement	Control Enhancements	Related ITSG-33 Controls
SC-2	Application partitioning	(A) The information system separates user functionality (including user interface services) from information system management functionality.	**Interfaces for non-privileged users:** The information system prevents the presentation of information system management-related functionality at an interface for non-privileged users. See related security control AC-3.	AC-3 SA-4 SA-8 SC-3
SC-3	Security function isolation	(A) The information system isolates security functions from non-security functions	**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.	AC-2 AC-6 SA-4 SA-5 SA-8 SA-13 SC-2 SC-7 SC-39
SC-7	Boundary Protection	(A) The information system monitors and controls communications at the external boundary of the system and at key internal boundaries within the system. (B) The information system implements sub-networks for publicly accessible system components that are [Selection: physically; logically] separated from internal organizational networks. (C) The information system connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.	**External telecommunications systems:** i. The organization implements a managed interface for each external telecommunication service. ii. The organization establishes a traffic flow policy for each managed interface. iii. The organization protects the confidentiality and integrity of the information being transmitted across each interface.	AC-4 AC-17 CA-3 CM-7 CP-8 IR-4 RA-3 SC-5

			iv. The organization documents each exception to the traffic flow policy with a supporting mission/business need and duration of that need. v. The organization reviews exceptions to the traffic flow policy [Assignment: organization-defined frequency] and removes exceptions that are no longer supported by an explicit mission or business need. **Deny by default and allow by exception:** The information system at managed interfaces denies network communications traffic by default and allows network communications traffic by exception (i.e., deny all, permit by exception). **Prevent split tunnelling for remote devices:** The information system, in conjunction with a remote device, prevents the device from simultaneously establishing non-remote connections with the system and communicating via some other connection to resources in external networks. **Route authenticated traffic to proxy servers:** The information system routes [Assignment: organization-defined internal communications traffic] to [Assignment: organization-defined external networks] through authenticated proxy servers at managed interfaces. **Restrict threatening outgoing communications traffic:** i. The information system detects and denies outgoing communications traffic posing a threat to external information systems. ii. The information system audits the identity of internal users associated with denied communications. **Prevent unauthorized exfiltration:** The organization prevents the unauthorized exfiltration of information across managed interfaces.	SC-13

			Restrict incoming communications traffic: The information system only allows incoming communications from [Assignment: organization-defined authorized sources] routed to [Assignment: organization-defined authorized destinations]. **Host-based protection:** The organization implements [Assignment: organization-defined host-based boundary protection mechanisms] at [Assignment: organization-defined information system components]. **Isolation of security tools, mechanisms, and support components:** The organization isolates [Assignment: organization-defined information security tools, mechanisms, and support components] from other internal information system components by implementing physically separate sub-networks with managed interfaces to other components of the system. **Protects against unauthorized physical connections:** The organization protects against unauthorized physical connections at [*Assignment: organization-defined managed interfaces*]. **Prevent discovery of components and devices:** The information system prevents discovery of specific system components composing a managed interface. **Automated enforcement of protocol formats:** The information system enforces adherence to protocol formats. **Fail secure:** The information system fails securely in the event of an operational failure of a boundary protection device.	

			Blocks communication from non-organizationally configured hosts: The information system blocks both inbound and outbound communications traffic between [Assignment: organization-defined communication clients] that are independently configured by end users and external service providers. **Dynamic isolation and segregation:** The information system provides the capability to dynamically isolate/segregate [Assignment: organization-defined information system components] from other components of the system. **Isolation of information system components:** The organization employs boundary protection mechanisms to separate [Assignment: organization-defined information system components] supporting [Assignment: organization-defined missions and/or business functions]. **Separate subnets for connecting to different security domains:** The information system implements separate network addresses (i.e., different subnets) to connect to systems in different security domains. **Disable sender feedback on protocol validation failure:** The information system disables feedback to senders on protocol format validation failure.	
SC-32	Information system partitioning	The organization partitions the information system into [Assignment: organization-defined information system components] residing in separate physical domains or environments based on [Assignment: organization-defined circumstances for physical separation of components].	None	AC-4 SA-8 SC-2 SC-3 SC-7

A.2 Management security controls

A.2.1 Risk assessment

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

Table 3: ITSG-33 risk assessment security controls: RA-2

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 GC 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