Communications Security Establishment
Centre de la sécurité des télécommunications

CANADIAN CENTRE FOR
CYBER SECURITY

Protecting your organization from software supply chain threats

Management

© Government of Canada
This document is the property of the Government of Canada. It shall not be altered, distributed beyond its intended audience, produced, reproduced or published, in whole or in any substantial part thereof, without the express permission of CSE.

ITSM.10.071

TLP:CLEAR

Canada

Foreword

This document is an UNCLASSIFIED publication that has been 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 February 8, 2023.

Revision history

Revision	Amendments	Date
1	First release.	Feb 8, 2023

ISBN 978-0-660-45701-7
CAT D97-4/10-071-2022E-PDF

Overview

Supply chain attacks are evolving threats that target third-party software suppliers. A software supply chain attack occurs when a cyber threat actor compromises the software before the supplier sends it to their customers. One successful intrusion can have a ripple effect and can potentially impact thousands of victims.

A threat actor can exploit the trusted relationship between the customer and the software supplier to gain privileged and persistent access to their victims' networks. Depending on the threat actor's intention and skills, they may be able to access customer's sensitive data for prolonged periods of time without being detected. Compromised systems often go undetected until significant damage has been done.

In this document, we will discuss the software supply chain security risks, why it matters, and what the customer can do to avoid becoming a victim of a software supply chain attack. Regardless of the size of your organization, if you are engaged with software suppliers, you will need to consider the risks of a software supply chain and take the necessary steps to identify, assess, and mitigate these risks. To effectively manage software supply chain risks, you need to incorporate software supply chain security practices in your IT security program and risk management framework.

Table of contents

List of figures

1 Introduction

Supply chains include each phase that transform raw materials, components, and resources into a specific product, as well as the delivery process to reach the end user. The entities in the supply chain include designers, developers, suppliers, warehouses, distribution centers, and retailers. In software, the raw materials are the common libraries, code, hardware, and tools that transform code into a final product. This product can be deployed as either an application for the end-user, or as a dependency used for a different product.

Software consumers need to understand that all software has vulnerabilities and can be exploited by a threat actor to alter its security properties and functionality for malicious intent. Unlike physical electronics and IT systems which are seldomly modified once they've left the production line, software is continuously being revised, updated, and patched. This makes the supply chain for software vulnerable to malicious additions at any point in its lifecycle.

There are several ways to attack a software supply chain, from direct insertion of malicious code into the source code of a software, or by taking over a developer's account to do so without others noticing, or by compromising a signing key to distribute software that isn't officially part of a component. Poor security practices at any point in the software supply chain lifecycle can lead to increased cybersecurity risk to the organization.

Developers will often use a variety of open-source software components and dependencies to create their programs and applications. Having access to free libraries, frameworks, and processes saves developers the time and cost of writing their code from scratch. For this reason, using open-source software has become standard practice in the application development process. The drawback to using open-source software to create code is the wide range of access and the ability for anyone to potentially make changes to it. As a result, programs and applications developed using open-source can have vulnerabilities that developers are unaware of and can pose significant security risks. Proprietary software can also have vulnerabilities if the developers are not following secure development practices.

The *Cyber Centre's National Cyber Threat Assessment 2023-2024* [1] notes that instead of targeting organizations directly, cyber threat actors are increasingly targeting the software tools and services used by organizations via supply chain compromises. The threat from supply chain compromises increases where vendors have elevated access to their clients' networks. This kind of relationship is becoming more common as cloud-based software, infrastructure, and platform "as-a-service" models proliferate.

To protect your organization from software supply chain attacks, you should incorporate risk management and security measures to address risks inherent to your software supply chain. The guidance in this document aligns with the risk management activities described in *ITSG-33 IT - Security Risk Management: A Lifecycle Approach* [2] as well as its associated publications *ITSM.10.089 - Top 10 IT security actions to protect Internet connected networks and information* [3] and *ITSAP.10.035 - Top measures to enhance cyber security for small and medium organizations* [4]. For more information on security controls, we also recommend reviewing the publication *Baseline Cyber Security Controls for Small and Medium Organizations* [5] as a starting point for improving your resilience to cyber threats.

2 Threats to the software supply chain

Whether it is to install updates or repair software vulnerabilities, there is ongoing communication between third-party software providers and their clients' networks. A threat actor can exploit this frequent communication to send malicious updates or block patches from being applied to exploit the unpatched vulnerabilities. If your organization falls victim to a compromise in the software supply chain, this can impact the confidentiality, integrity, and availability (the three pillars of IT security) of your organization's information systems and assets. It is imperative to remember that your organization is legally responsible for protecting its information, even when you are using third-party services.

Ultimately, software supply chain compromises have the same potential effect as any cyber compromise (data exfiltration, surveillance, ransomware, etc.). The difference is that supply chain compromises are difficult to prevent due to the lack of control you have over your software suppliers' security controls. A single upstream compromise can be used to pivot into many downstream client networks.

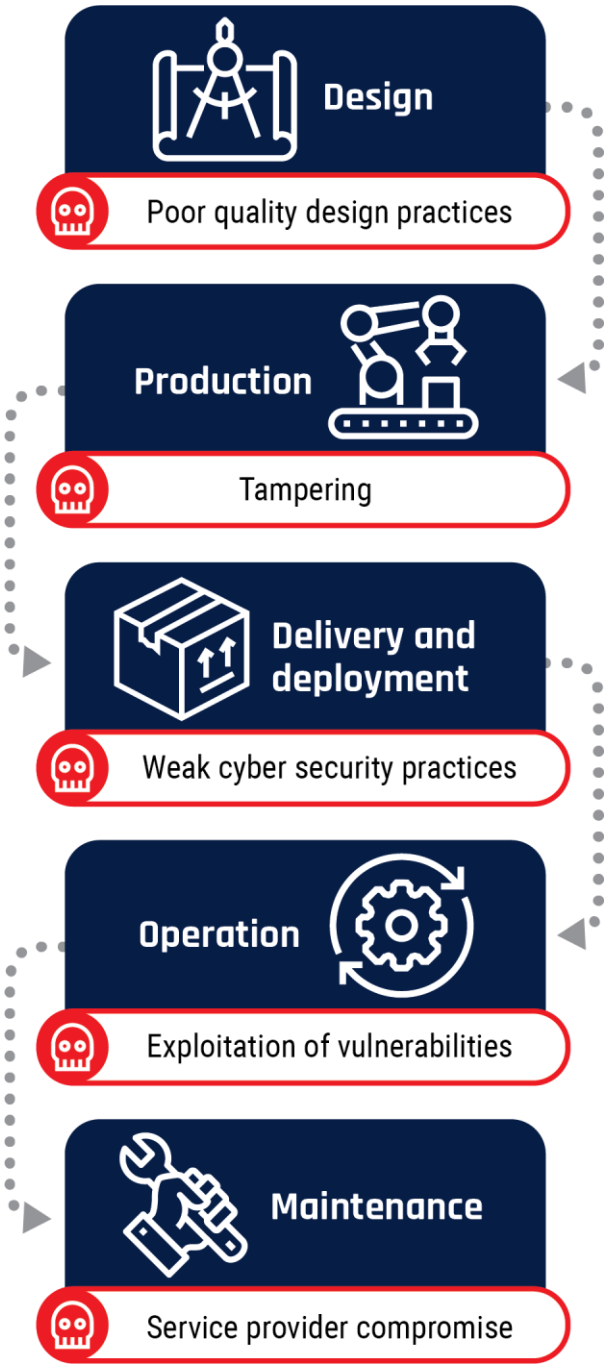
A threat actor can exploit the trusted relationship between organizations and software vendors to gain privileged and persistent access to their victims' networks. Depending on the threat actor's intentions and skills, they may be able to access your organization's sensitive data for prolonged periods of time without being detected. Compromised systems often go undetected until significant damage has been done. This can be destructive to your organization's reputation and credibility as the threat actor can perform various malicious activities such as:

- Monitoring organizational communications and actions
- Stealing data, financial and proprietary information
- Disabling networks or systems, and more

2.1 Software supply chain lifecycle (SCL)

Software supply chains fall under the ICT supply chain lifecycle. As demonstrated in Figure 1, the ICT SCL has five phases, and this is no different for software SCL. Figure 1 shows that a security weakness at any of these phases: design, production, delivery and deployment, operation, and maintenance, can give the threat actor the opportunity to carry out malicious activities and compromise the software.

Figure 1: Supply chain lifecycle



2.1.1 Examples of successful attacks at the different stages of the SCL

SolarWinds is an IT management company whose build server, which is a dedicated machine used for building applications, was infiltrated by a foreign threat actor in 2020. The threat actor remained undetected in SolarWinds' network for months before inserting malware into the software update process to infiltrate and infect customer networks. This is an example of a compromise in both the production and maintenance phases of the SCL. When hijacking updates or devices, the threat actor can insert malware or alter the original update to capture system control.

In December 2021, a critical vulnerability was discovered in Log4j, an open-source logging library commonly used by millions of computers worldwide running software applications and online services. This is a perfect example of an open-source vulnerability and if left unfixed, attackers could have breached systems, stollen passwords and login credentials, extracted data, and infected networks with malicious software. Many Canadian organizations and federal agencies had to shut down their websites and service infrastructures as a precautionary measure. The quickest recommended mitigation response was to upgrade all instances of Log4j to the latest version. This was to help reduce future attacks but would not remediate any damage caused before the library upgrade. Because this vulnerability was so widespread, it was assumed that an organization's ecosystem was compromised prior to a library upgrade and a data breach incident response needed to be initiated immediately.

The list below provides more examples of successful attacks at the different stages of the ICT SCL. Several other examples and further information on these attacks can be found in the National Institute of Standards and Technology (NIST) publication *Defending Against Software Supply Chain Attacks* [6] and National Counterintelligence and Security Center (NCSC) publication *Software Supply Chain Attacks* [7].

1. GoldenSpy is malware hidden in a tax software [8]. In 2020, an identified piece of malware was discovered embedded in tax payment software that some foreign businesses operating in China were required to install.

    - Entry point: Built software with hidden malware
    - Phase of the SCL: Design phase

2. ShadowHammer attack was a sophisticated supply chain attack involving ASUS Live Update Utility [9]. In 2019, at least six IT infrastructures were infiltrated. A sophisticated group of threat actors modified an old version of the ASUS Live Update Utility software and pushed out the tampered copy to ASUS computers around the world.

    - Entry point: Compromised production infrastructure
    - Phase of the SCL: Production phase

3. In 2017, a Moscow-based antivirus vendor, Kaspersky Lab, was being used by a foreign intelligence service to secretly scan computers around the world for classified U.S. government documents and top-secret information [10]. U.S. government customers were told to stop using this vendor's products and were banned from acquiring future products.

    - Entry point: Compromised software used as an espionage tool
    - Phase of the SCL: Delivery and deployment phase

4. In 2020, a threat actor targeting the Vietnamese Government Certification Authority (VGCA) compromised the agency's digital signature toolkit [11]. A threat actor exploited the software installers hosted on the VGCA's website to inject spyware known as PhantomNet or Smanager.

    - Entry point: Compromised digital certification authority website
    - Phase of the SCL: Operation phase

5. In 2021, a ransomware group inserted malicious code into an update for Kaseya's Virtual System Administrator (VSA) software [12]. After updating, hundreds of companies found their systems were inaccessible due to ransomware.

    - Entry point: Software update
    - Phase of the SCL: Maintenance phase

2.2 Common software supply chain attack vectors

A software supply chain attack is seldomly the end goal of the threat actor. It is an opportunity for the threat actor to infiltrate numerous networks to compromise the operations of several organizations. The following section details the most common attack vectors used for software supply chain attacks.

2.2.1 Compromised updates

Vendors disseminate software to offer their customers bug and security patches which are important for their software's continued functioning and safety. A threat actor can use the update mechanisms to distribute malware to unwary users, specifically when the threat actor has compromised the developer's network. Given that there are no policies or standards for software update processes, without the digital signature, there is no way for users to validate or verify the integrity of the update issued and downloaded. It validates the authenticity and integrity of the software upon installation and execution.

When updating your software using a network connection, a threat actor can intercept the update and send malware to gain control over the software's normal functionality.

2.2.2 Open-source software components and dependencies

The use of open-source software components and dependencies to create code is on an upward trend with developers. Open-source software is found in online software libraries or repositories where users can install the latest versions and updates of software. Many developers choose to work with open-source software as it saves them from having to develop standard capabilities themselves. Open-source software also saves developers resources, as the software and updates are free of charge. There are risks associated with using these software components, especially when they are no longer being maintained and patched. If a cyber threat actor gains access to these open-source repositories, they can deliver compromised versions of software without the developers' knowledge and potentially gain unauthorized access not only to the developers' network, but also to downstream software users' networks, systems, and sensitive data. More and more developers are being asked to validate the integrity of their product by providing an inventory, or a software bill of materials (SBOM), of all components used to create their product. A SBOM will ensure that the licensing obligations of those components are being met and that patches are being applied when necessary.

2.2.3 Code signing keys

Code signing is a cryptographic method used by developers to create digital signatures to prove the integrity of the software. The digital signature provides proof to end-users that the code has not been tampered with while making its way from the

supplier. This is especially important when downloading software from third-party websites rather than the supplier themselves.

Threat actors sabotage code signing by using the following methods:

- Using self-signed certificates which are public key certificates that are not signed by a publicly trusted certificate authority (CA) but by one's own private key
- Breaking signing systems
- Manipulating misconfigured account access controls
- Purchasing stolen certificates
- Compromising the signing infrastructure and issuing seemingly legitimate certificates

3 Software security best practices for your organization

We recommend you follow the actions listed in this section to help assist you in selecting the right suppliers and to maintain a strong cyber security posture when using software and applications.

1. **Research the suppliers**: You should research the suppliers to better understand how they operate. Ask them about the certifications, security standards, and processes they have in place to verify whether they can support your business needs and security requirements. Another consideration is the potential sponsorship or affiliation with state actors that may have ulterior motives when engaging in a service level agreement with your organization.
2. **Identify roles:** Work with your vendors and suppliers to clearly define roles, responsibilities, and processes for reporting and responding to security incidents in the supply chain. A good relationship with your vendors will ensure that updates or changes to processes are communicated and that robust incident response and mitigation processes are implemented in a timely manner.
3. **Document your software security and acquisition policies:** In addition to relying on the vendors' self-certification, which often relies on questionnaires to perform due diligence, you should conduct your own audits, source code reviews, and penetration testing. You should also maintain an inventory of your organization's current and future software licenses.
4. **Monitor your suppliers:** Static monitoring isn't enough to protect your data and networks from a threat actor who may be targeting the software and applications running on your networks. Establish monitoring parameters that will allow for continuous monitoring of your vendors and their security controls that impact your organization.
5. **Know when to update and patch your software:** Updates and patches should not be implemented until the vendor confirms that no issues were identified in pre-production testing.
6. **Strengthen security access control and authorization**: Your organization should use the principle of least privilege by assigning users the minimum level of access required to perform their job. Enforcing the principle of least privilege significantly reduces your attack surface by eliminating unnecessary access rights, which can lead to a variety of compromises.
7. **Securing your contracts:** Include security, privacy, document management, and compliance requirements in every request for proposal (RFP) and supplier contract.
8. **Educate and train your employees on software security.** Having a well-organized and established security training program for your employees is essential to ensure success in protecting your organization from cyber threats. Employee training should be conducted on a regular basis. For more information on training, you can reference *ITSM.10.093 - Top 10 IT security actions: #6 provide tailored cyber security training* [13].
9. **Implementing an incident response (IR) plan**. No matter how proactive you are when it comes to software security best practices, there is always a possibility of a breach. Being prepared can stop a threat actor from achieving their mission, even after you've been breached, by limiting the damage.
10. **Strengthening network monitoring and logging:** Network monitoring and logging will detect unusual behaviour patterns and track if system changes.

3.1 Vetting software suppliers

With the array of software suppliers available, you may find it challenging to properly vet a supplier. The following is a list of a few parameters you can use to assess the security compliance of potential software suppliers.

1. Are they using a secure software development lifecycle (SSDL) framework and is it documented?
2. Do they have a document process to prove that the activities described in the SSDL occur as expected?
3. Do they incorporate security practices at every stage of the software development lifecycle?
4. Are strong security standards and controls applied at every stage of the development lifecycle to monitor and manage the production processes?
5. Do they have a fulltime knowledgeable software security team?
6. Are the team members educated on secure software development, open-source security, and DevSecOps practices?
7. Do they perform employee background checks?
8. Do they only use developers who keep detailed records of the dependencies used in their software? Are the developers keeping up to date with the latest versions of their library dependencies?
9. Is the mitigation of known vulnerabilities factored into product design?
10. Are they staying current on new evolving vulnerabilities? Do they get alerted to vulnerability disclosures?
11. Do they have a well documented system for patching security flaws and fixing security defects?
12. Are vulnerabilities actively identified and disclosed? Do they have a vulnerability response program and team in place?
13. Are their software security activities and products reviewed by a third-party?
14. Do they have a software configuration management (SCM) process in place to track, manage, and control the changes in the software/codes during the software development lifecycle?
15. Can they ensure that your organization's data will be protected? Do they use data encryption, and do they dispose of the data when the relationship with their clients is completed?
16. Do they have internal auditing procedures for all their security operations?
17. Can they confirm software integrity by using a code authentication mechanism?
18. Does the vendor have a software component inventory or a software bill of material (SBOM) to track components, and audit their controls to keep software secure? What details are included in the SBOM?
19. Does the vendor have protocols for how to notify appropriate stakeholders in the event of a vendor breach?

4 Supply chain risk management considerations for large organizations and critical infrastructures

Identifying, assessing, and mitigating cyber supply chain risks is imperative for critical infrastructures and organizations. It allows them to foster resiliency and protection against cyber incidents. The multidisciplinary approach to managing these types of risks to the cyber supply chain is called cyber supply chain risk management (C-SCRM). Software supply chain security goes hand in hand with C-SCRM. It is important for large organizations and critical infrastructures to implement the security controls, audits, and risk management policies and processes needed to help mitigate their supply chain risks. This will allow them to maintain their information and systems' confidentiality, integrity, and availability.

Integrating software into the C-SCRM framework will help organizations understand the risks presented by software. Organizations can manage these risks by identifying various technical and non-technical requirements for C-SCRM in relation to software. Establishing a risk management framework tailored to their organization will help ensure the secure supply of software applications and how they are managed at every phase of their lifecycle. A risk management plan that incorporates software is a significant component of any organization's overall cyber security strategy.

Here are a few preliminary steps that are required to develop your C-SCRM:

1. Identify your key mission or business process and the essential services your organization provides
2. Understand your organization's security requirements
3. Define your organization's overall risk strategy and tolerance
4. Translate the risk and corresponding security requirements into a C-SCRM program

NIST suggests eight fundamental practices for developing a C-SCRM framework that can be applied to software. Following these actions will help prevent, mitigate, and respond to software vulnerabilities that may be introduced through the cyber supply chain and exploited by malicious actors.

1. Integrate the C-SCRM framework across your organization
2. Establish a formal C-SCRM program that is evaluated and updated in real-time
3. Know your critical suppliers and how to manage them
4. Understand your organization's supply chain
5. Closely collaborate with key suppliers and incorporate them in your supplier risk management program
6. Include key suppliers in resilience and improvement activities as part of your vendor risk assessment process
7. Assess and monitor the supplier relationship by providing continuous monitoring of your C-SCRM
8. Plan for the full lifecycle of your asset

5 Fostering cyber security resiliency and improvement

Cyber resilience helps organizations prepare for, respond to, defend against, and recover from cyber attacks including software supply chain attacks. A cyber resilient organization can adapt to known and unknown crises and threats and ensures continued business operations despite adverse events.

It is now expected that it's no longer a matter of 'if' but 'when' an organization will suffer a cyber attack. Therefore, instead of focusing your efforts and resources on keeping threat actors out of your network, you should assume they will eventually break through your defences and start working on a strategy to reduce the impact.

5.1 Strengthening your organization's security posture

To stay cybersafe, we recommend that you use an IT security risk management framework such as *IT Security Risk Management: A Lifecycle Approach (ITSG-33)* [2], *ISO-27001 Information Security Management* [14], or *NIST SP 800-37 Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy* [15] to strengthen your organization's security posture. However, these profiles are expensive to implement and beyond the financial or human resources threshold of most small and medium organizations in Canada.

Organizations can mitigate most cyber threats through awareness and best practices in cyber security and business continuity. The Cyber Centre's publication *Baseline Cyber Security Controls for Small and Medium Organizations* [5] presents a condensed set of security controls to enhance the ability of organizations to get the most out of their cyber security investment. These security controls are taken from the security controls listed in *Annex 3A of ITSG-33* [2]. *ITSG-33* [2] describes the roles, responsibilities, and activities that help organizations manage their IT security risks and includes a catalogue of security controls (i.e. standardized security requirements to protect the confidentiality, integrity, and availability of IT assets). These security controls are divided into three classes, which are further divided into several families 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 managing IT security and IT security risks.

These controls will provide your organization with the tools to:

- Manage and protect your information and systems by identifying, assessing, and managing the risks associated with network and information systems, including those across the supply chain.
- Identify and detect anomalies and potential cyber security incidents before they cause damage through continual monitoring of your network and information systems.
- Develop a contingency plan for implementing alternate software in the case of cyber security incidents.
- Respond to and recover from cyber incidents to ensure business continuity.

5.2 Ensuring business continuity

To ensure continued operations with minimal downtime, we recommend that you have an IT recovery plan [16] as part of your overall business continuity and risk management framework. Your organization should identify critical data, applications, and processes and define how it will recover IT services that support business operations, products, and services.

Your recovery plan should clearly identify and document what is to be recovered, by whom, when, and where. In general, there are two types of plans you should consider developing for your business.

1. **Disaster Recovery Plan:** The primary goal is to ensure business continuity during an unplanned outage or service disruption. For more information on how to develop a recovery plan refer to *Developing your IT recovery plan (ITSAP.40.004)* [16].
2. **Incident Response Plan:** The primary goal is to protect sensitive information during a security breach. For more information on how to develop and incident response plan refer to *Developing your incident response plan (ITSAP.40.003)* [17].

These two plans take into consideration two major events that could cause an unplanned outage and require you to activate your recovery response.

Your IT recovery plan should be tested to identify inconsistencies and provide opportunities to address areas that require revision. It is recommended you test your organization's IT recovery plan in a test environment to avoid business interruptions.

6 Summary

This document discusses software supply chain security risks and why it matters. Organizations should follow the software security best practices to avoid software supply chain attacks. Additionally, a list of parameters to help organizations select the right suppliers and to assess the suppliers' security compliance has been included in this document. It is recommended that organizations incorporate these software security practices in their IT security program and risk management framework to create a more cyber resilient organization and ensure continued business operations despite adverse events.

7 Supporting content

7.1 List of abbreviations

Term	Definition
CA	Certificate Authority
CSE	Communications Security Establishment
C-SCRM	Cyber supply chain risk management
DoS	Denial of service
GC	Government of Canada
ICT	Information and communications technology
ISO	International Organization of Standardization
NIST	National Institute for Standards and Technology
IT	Information Technology
ITS	Information Technology Security
RFP	Request for Proposal
SBOB	Software bill of materials
SCL	supply chain lifecycle
SSDL	Secure software development lifecycle
NCSC	National Cyber Security Centre
VGCA	Vietnamese Government Certification Authority
VSA	Virtual System Administrator

7.2 Glossary

Term	Definition
Availability	The ability for the right people to access the right information or systems when needed. Availability is applied to information assets, software, and hardware (infrastructure and its components). Implied in its definition is that availability includes the protection of assets from unauthorized access and compromise.
Compromise	The intentional or unintentional disclosure of information, which adversely impacts its confidentiality, integrity, or availability.
Confidentiality	The ability to protect sensitive information from being accessed by unauthorized people.
Cyber attack	The use of electronic means to interrupt, manipulate, destroy, or gain unauthorized access to a computer system, network, or device.

Term	Definition
Cyber threat	A threat actor, using the Internet, who takes advantage of a known vulnerability in a product for the purposes of exploiting a network and the information the network carries.
Cyber Security	The ability to protect or defend the use of cyberspace from cyber attacks.
Data	Electronic representation of information. The quantities, characters, or symbols on which operations are performed by a computer, being stored, and transmitted in the form of electrical signals and recorded on magnetic, optical, or mechanical recording media.
Hacker	Someone who uses computers and the Internet to access computers and servers without permission.
Integrity	The ability to protect information from being modified or deleted unintentionally or when it is not supposed to be. Integrity helps determine that information is what it claims to be. Integrity also applies to business processes, software application logic, hardware, and personnel.
Information and communications technology (ICT)	All technical means used to handle information and aid communication. This includes both computer and network hardware, as well as software.
Information technology (IT)	Technology that involves both technology infrastructure and IT applications.
IT Security	The discipline of applying security controls, security solutions, tools, and techniques to protect IT assets against threats from compromises throughout their lifecycle, based on the security category of supported business activities, and in accordance with departmental and GC policies, directives, standards, and guidelines.
Malware	Malicious software designed to infiltrate or damage a computer system, without the owner's consent. Common forms of malware include computer viruses, worms, Trojans, spyware, and adware.
Organization	An entity of any size, complexity, or positioning within an organizational structure (e.g. a federal agency or, as appropriate, any of its operational elements).
Risk	A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence.
Risk assessment	The process of identifying, estimating, and prioritizing risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the nation, resulting from the operation of an information system.
Risk management	The continuous, proactive, and systematic process of identifying, assessing, understanding, acting on and communicating risk.

Term	Definition
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.
Supply chain	Supply chain refers to the processes required to design, manufacture and distribute equipment or other commodities, including information technology hardware and software [1].
Threat actors	Threat actors are states, groups, or individuals who, with malicious intent, aim to take advantage of vulnerabilities, low cyber security awareness, or technological developments to gain unauthorized access to information systems in order to access or otherwise affect victims' data, devices, systems, and networks.
Vulnerability	A flaw or weakness in the design or implementation of an information system or its environment that could be exploited to adversely affect an organization's assets or operations.

7.3 References

Number	Reference
1	Canadian Centre for Cyber Security. *National Cyber Threat Assessment 2023-2024*.
2	Canadian Centre for Cyber Security. *ITSG-33 IT Security Risk Management: A Lifecycle Approach.* November 2018.
3	Canadian Centre for Cyber Security. *ITSM.10.089 Top 10 IT security actions to protect Internet connected networks and information.* September 2021.
4	Canadian Centre for Cyber Security. *ITSAP.10.035 Top measures to enhance cyber security for small and medium organizations*. June 2021.
5	Canadian Centre for Cyber Security. *Baseline Cyber Security Controls for Small and Medium Organizations*. May 2021.
6	National Institute for Standards and Technology. *Defending Against Software Supply Chain Attacks.* April 2021.
7	The National Cyber Security Centre. *Software Supply Chain Attacks.* March 2021.
8	Darkreading. *GoldenSpy' Malware Hidden in Tax Software Spies on Companies Doing Business in China*. June 2020.
9	Securelist. *Operation ShadowHammer: a high-profile supply chain attack*, April 2019.
10	The Wall Street Jounal. *Russia Has Turned Kaspersky Software into Tool for Spying*. October 2017.
11	The Hacker News. *Software Supply-Chain Attack Hits Vietnam Government Certification Authority.* December 2020.

Number	Reference
12	Secpod *Kaseya's Virtual System/Server Administrator (VSA) Zero-Day Under Active Exploitation By REvil Ransomware*. July 2021.
13	Canadian Centre for Cyber Security. *Top 10 IT security actions: #6 provide tailored cyber security training ITSM.10.093*. February 2020.
14	International Organization for Standardization. *ISO 27001: Information Security Management*. 2018.
15	National Institute of Standards and Technology. *Special Publication Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*. 2018.
16	Canadian Centre for Cyber Security. *Developing your IT recovery plan ITSAP.40.004*. January 2021.
17	Canadian Centre for Cyber Security. *Developing your incident response plan ITSAP.40.003*. May 2021.