ESTABLISHING AN ENTERPRISE CYBER SECURITY PROGRAM: A GUIDE FOR CANADIAN ROAD INFRASTRUCTURE OWNER/OPERATORS AND ITS PROFESSIONALS

2026

Transports Canada Transport Canada

Canada

This guide assists road authorities and infrastructure owners and operators in developing and maturing an intelligent transportation systems (ITS) cyber security program.

Aussi disponible en français sous le titre : « Établir un programme de cybersécurité intégrée : Guide pour les propriétaires/exploitants d'infrastructures routières canadiennes et les professionnels des STI »

TP 15628E

Cat. T89-24/2025E-PDF

ISBN 978-0-660-75822-0

Table of contents

Acronyms and abbreviations

Below is a list of acronyms used in this guide. Each term is spelled out in full the first time it appears in the main text, followed by its acronym for subsequent uses.

CCCS – Canadian Centre for Cyber Security

CMMI – Capability Maturity Model Integration

DDoS – Distributed denial of service

DoS – Denial of service

ERM – Enterprise risk management

IOO – Infrastructure owners and operators

IoT – Internet of Things

IT – Information technology

ITS – Intelligent transportation systems

KPI – Key performance indicator

NIST – National Institute of Standards and Technology

OT – Operational technology

PIPEDA – Personal Information Protection and Electronic Documents Act

TMS – Transportation management system

Executive summary

Intelligent transportation systems (ITS) are transforming road transportation by improving safety, efficiency, and mobility through increased connectivity, automation, and data exchange. At the same time, this growing reliance on digital technologies has expanded the cyber threat landscape, exposing transportation infrastructure to risks that can impact public safety, disrupt operations, damage organizational reputations, or result in financial losses. As a result, cyber security is now a core component of resilient and trustworthy transportation systems.

This guide supports Canadian road authorities and infrastructure owners and operators (IOOs) in their efforts to establish, strengthen, or sustain an ITS cyber security program. It provides practical, step-by-step guidance for managing cyber risks in environments where information technology (IT), operational technology (OT), and safety-critical systems increasingly converge, and is centred on a structured seven-step process for creating or improving a cyber security program. The guidance aligns with the National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity and emphasizes a risk-based, maturity-driven approach.

This guide is not intended to be exhaustive or prescriptive. Rather, it is designed to complement existing standards and guidance from trusted authorities, including Public Safety Canada and the Canadian Centre for Cyber Security (CCCS). By applying the principles and steps outlined in this guide, organizations can strengthen the resilience of their ITS, better protect public safety and data, and support the secure deployment of current and future transportation technologies.

Introduction: Securing an evolving cyber threat landscape and scope of this guide

Technology in road transportation is evolving rapidly, enhancing safety, mobility, and efficiency for all transportation system users. However, these advancements can also introduce new cyber security risks. In the past, cyber security protection measures focused heavily on isolating networks and creating a hard perimeter to prevent threats from breaching an organization's defenses. While this approach is still important, cyber security now requires organizations to develop new ways to prevent, respond to and recover from a wider range of increasingly sophisticated threats. As the cyber threat landscape expands, securing intelligent transportation systems (ITS) is becoming an increasingly important priority.

This guide is intended to help road authorities and infrastructure owners and operators (IOOs) to develop and mature an ITS cyber security program. It provides guidance on:

- how to set up a cyber security program
- how to create a plan for maturing your organization's cyber security posture
- common controls that your organization can put in place.

It is designed to align with the National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity.

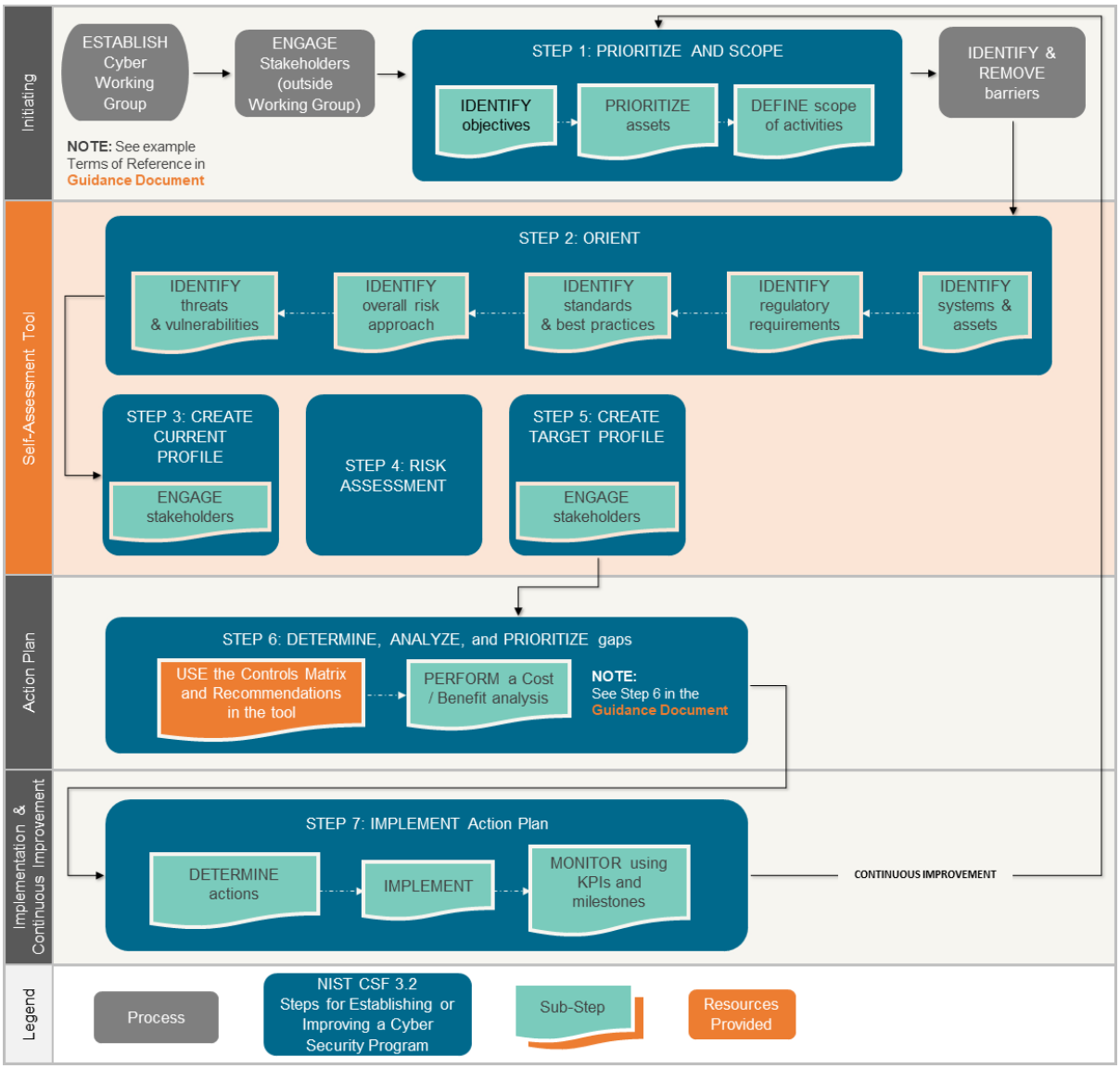
As illustrated in Figure 1 (below), the program setup consists of seven steps organized into four distinct phases. The section "How to create or improve a cyber security program" follows this sequence directly to assist with implementation. Because maintaining resilience requires ongoing commitment, these steps are designed to be iterative, enabling your organization to continuously refine its security posture over time.

While this document serves as a foundational guide, it should be used in conjunction with the latest best practices from Public Safety Canada, the Canadian Centre for Cyber Security (CCCS) and trusted international regulators.

This guide complements other resources that are available on Transport Canada's road infrastructure cyber security web page, including:

- **ITS Cyber Security Briefing Document:** A high-level briefing for road infrastructure executives on the importance of investing in cyber security resilience
- **ITS Cyber Security FAQ**: An FAQ webpage to answer common questions about managing cyber risks and strengthening the cyber resilience of ITS
- **ITS Cyber Security Self-Assessment Tool:** A spreadsheet-based tool with a current profile assessment questionnaire and target profile assessment questionnaire, which can be used to generate pragmatic recommendations and actions to enhance your organization's cyber posture. The Tool is accompanied by a User Guide. You are required to provide an email address to download both the Tool and the User Guide
- **Road Infrastructure Operational Technology Cyber Security Primer:** Provides basic guidance and best practices to help you design and implement a cyber security program

Figure 1: Overview of the steps to create or improve a cyber security program



Cyber security challenges in connected and converging ITS environments

Today's transportation management system (TMS) landscape is heavily interconnected to enable efficient and safe management of transportation resources. ITS are an integration of road transportation infrastructure, vehicles, and communications.

A byproduct of this interconnection can be a blurring of the lines between traditionally isolated operational technology (OT) and highly connected information technology (IT) environments. This is referred to as convergence, and without proactive measures, can expose your ITS to new vulnerabilities and a wider threat landscape.

A traditional TMS comprises multiple components, such as signal controllers, traffic sensors, closed-circuit television, and variable message signs. Many legacy and existing components in a TMS were not typically intended to be connected to external networks. As a result, standard security controls that are common to IT systems, such as mandatory authentication and authorization, were not prioritized during their development. The lack of basic security controls poses a potential risk when integrating legacy TMS infrastructure with modern ITS. Because ITS introduces external connectivity to previously air-gapped devices, understanding the existing TMS architecture and identifying potential security gaps is essential to reducing risk exposure prior to integration.

Another challenge that ITS operators must consider is interoperability. Many infrastructure environments consist of old and new systems or platforms that coexist and interact. Customized connectivity solutions and integrations are common in these environments and can be challenging to keep secure with the latest security patches – if these are even available.

Furthermore, a TMS gathers and sends large amounts of data to various endpoints and through connected devices. This data is what keeps the TMS operating correctly, efficiently, and safely. Endpoint devices that send and receive data within a TMS are often Internet of Things (IoT) devices with inherent exposure to the internet. These IoT devices may not be sufficiently hardened prior to deployment. As a result, the data or operational integrity of these components can be compromised or manipulated.

Key cyber security risks

Safety - Cyber threats targeting traffic signals, surveillance systems, or emergency infrastructure, such as 9-1-1 and incident detection systems, could pose serious safety risks for commuters and road operators.

Transportation infrastructure should be developed with enhanced measures to maintain the safety of riders, commuters, and workers. If safety systems and their fail-safes were compromised, riders, commuters, and operators could be put at risk of injury or death. Since safety systems are targets that provide significant leverage to attackers, they should be thoroughly protected.

Operational disruption - Cyber attacks can lead to traffic slowdowns, shutdowns, and congestion, affecting the efficiency of transportation networks and disrupting supply chain movements. For example, a targeted attack could result in the loss of function in a lane control system, which will lead to increased congestion, the potential for traffic accidents, and disruptions to major transport routes.

Reputation damage - A security breach or disruption could damage the reputation of the affected organization and may reduce public support for connected transportation technologies more broadly.

In situations where there is a data breach containing personal information, such as names, addresses or other sensitive information, there may be important privacy risks for the public (i.e. fraud and identity theft), and damage to the organization's reputation. Privacy data should be protected appropriately, and your organization should understand the applicable legislative requirements for handling data, such as the Personal Information Protection and Electronic Documents Act (PIPEDA), the *Privacy Act*, and/or any relevant provincial privacy legislation or organizational requirements.

Financial consequences - Ransomware attacks, regulatory fines, and legal liabilities can result in significant financial losses. This may come in many forms, whether it is paying the extortion value an attacker requests (ransomware), legal costs, reputational harm or infrastructure damage.

How to create or improve a cyber security program

Developing a cyber security program will take time, effort, and resources. This can be challenging as individuals and subject matter experts will likely have other responsibilities within the organization. However, the benefit of a well-developed cyber security program outweighs the cost. It's important that those developing the cyber security program have the appropriate amount of time and management support to do so – this should not become a low priority initiative. The Cyber Security FAQ also addresses some common questions relating to considerations for smaller or more resource-constrained IOOs.

Prior to launching a cyber security program, you should establish a **cyber security working group,** which is described below. Following the establishment of the working group, we will present seven (7) steps to create a cyber security program. Note that in the text of these steps, when we refer to "you", we are referring to the working group at your organization.

Establish a cyber security working group as a foundation to a cyber security program

A dedicated **cyber security working group** can promote a coordinated approach across the organization to cyber security.

This working group must be created to conduct (or start) the tasks, make decisions, and oversee the process.

The responsibilities of a cyber security working group usually include:

- signing off on acceptable cyber related risks
- approving third-party vendors
- approving cyber-related training material
- monitoring implementation of cyber programs or initiatives
- continuously measuring their organization's cyber maturity

There are several parts to a successful working group:

- the authority (technical and business) to make decisions related to the group's scope and mandate
- the ability to secure funding for the group's work
- representation from all impacted internal stakeholder groups, including IT, OT, and safety, and representation from multiple organizational levels including managerial, technical, and executive
- regular meetings that identify, assign, and track actions
- sharing information with the wider organization through regular updates and through training programs

Senior leadership endorsement of the cyber security working group is a critical aspect. It provides the group with credibility, access to resources, and a clearer path to making the necessary changes.

Appendix B of the ITS Cyber Security Self-Assessment Tool User Guide contains a sample Terms of Reference for a cyber security working group that includes a leadership endorsement.

Once created, the working group will become a force for *organizational change*, ensuring that the organization's cyber security maturity is measured, improved, and maintained through time.

There are many recognized models for organizational change, such as Kotter's model.

Eight activities for leading change[1] as part of the cyber security working group

1. Create a sense of urgency

Organizations and their leaders need to understand the urgency of the risks posed by cyber attacks.

This document provides background about the cyber threat landscape in Canada, and potential risks when adopting new digital technologies.

2. Build a guiding coalition

A successful cyber security program has wide ranging impacts on organizations, their people, and their processes. It is important to have support and guidance throughout the organization.

Stakeholders who are not part of the working group can be informed through meeting minutes, briefings, and other communications, such as newsletters and trainings, as needed.

3. Form a strategic vision

Identifying the group's strategic vision should be one of the first tasks of a working group. A clear vision will provide a roadmap for future activities and a view of what "success" means.

This is likely to be informed by the Terms of Reference of the group (see Appendix B of the ITS Cyber Security Self-Assessment Tool User Guide). Lower-level advice on how to identify initiatives is provided in subsequent sections of this guidance.

4. Build a network of security champions

Cyber security is too big a problem to be tackled by a single, dedicated group. To be scalable and effective, naming local security champions, who can identify and report issues, is key. This may require training and awareness campaigns. Where possible, look for people with existing cyber security expertise to join the working group.

5. Remove barriers

The working group should identify and target the key barriers to improving security. Barriers will vary from organization to organization and can include:

- siloed organizational structures
- incomplete or missing risk management practices
- lack of planning
- limited funding
- diffused accountabilities

6. Focus on short-term wins

Quick wins are an effective way to motivate groups, show progress and value.

More details on identifying actions for the group are listed below. It is important that the group measures and promotes successes to stakeholders.

---

[1] Kotter, John P. *8 Steps to Accelerate Change in Your Organization*. 2018

7. Keep at it

Cyber security is a fast-moving area and maintaining your security posture requires focus. Making ongoing progress will require the group to meet regularly and to ensure that actions are completed, celebrated, and promoted to stakeholders.

8. Stay agile

To maintain progress, you need to be comfortable with frequent change. This should be built into your organization's culture, but the changes should always be linked to your organizational objectives. You can accomplish this by measuring outcomes and performing before/after studies on organizational maturity.

Our ITS Cyber Security Self-Assessment Tool can support this work.

Common pitfalls of cyber security working groups

"Talking shop" – Lack of clear objectives

Cyber security is an interesting topic that enthusiasts will happily discuss at length. While this can be great for initial meetings, it is vital that this knowledge gets turned into tasks.

Agendas for working group meetings can help make sure that there is a balance between informative discussion and activity during meetings.

Fatigue

Attendance at working group meetings can begin to wane, especially if there are lengthy periods without visible progress. Maintaining momentum should be a key task for the working group's chair.

Establishing and monitoring key performance indicators (KPIs), discussing progress at meetings and celebrating milestones can help maintain momentum, while a lack of funding or recognition from management can hinder it.

Training and awareness can help make sure that members understand what's at stake. Regular "security moments" that explore how cyber security failures have impacted other businesses can help make sure that members understand the importance of the working group activities.

Not setting priorities

When tasks are assigned to working group members, it's important to remember that those members also have other work that's vying for their attention.

To prevent cyber tasks being forgotten, it's important not to overload group members. To help you prioritize tasks, each should be linked to business objectives or risks.

Step 1: Prioritize and define scope

Identifying your key objectives, such as system reliability, data integrity, and public safety, is vital to making sure that cyber security protections are linked to real-world needs.

The following are suggested as initial high-level objectives that you can use as a starting point, but the cyber security working group may have more specific ideas that can be captured and added to augment them:

- protecting the staff and the people using the transport network
- making sure the transport network is reliable for all users

Summary of step 1: Prioritize and define scope

- Identify key business objectives
- Define the scope of cyber program

To develop a cyber security program that reflects these goals, it's important to define the scope of the activities. A well-defined scope will not only give you an idea of the resources you will need, but will also provide the system boundaries to model in later stages.

Some factors to consider include:

- **the stage or maturity of the cyber security program** – for example: initial requirements definition, detailed design, development, final implementation stages, maintenance, and improvement
- **the risk environment** – assets and services at risk, networks, etc.
- **the purpose of the program** – major requirements for change will require a detailed assessment of scope, while high-level requirements would have a broader scope
- **cost and time constraints** – practical considerations may limit the scope[2]

The technical scope of the cyber security program for your organization won't be limited to IT systems. OT, safety systems, and embedded systems are likely to be just as important to the organization's stated goals.

Step 2: Orient

The "orient phase" is an opportunity to define the landscape in which the cyber security working group will operate. This includes identifying assets, connections, interfaces, and the legislative landscape, as well as understanding vulnerabilities and the threat landscape.

A foundational activity in this phase is developing a comprehensive inventory of assets within scope. An example output is an asset register of OT and IT system components. You can use the Asset Management portion of the NIST framework (See Appendix A 1.2 of the ITS Cyber Security Self-Assessment Tool User Guide) to create an

Summary of step 2: Orient

- Identify assets, connections, and interfaces
  - Create an information system model
- Understand legislative landscape
- Identify vulnerabilities
  - Secure vulnerability documentation

[2] Harmonized Threat and Risk Assessment (TRA) Methodology. (2007). MS-4

asset register. For software, you could create a software bill of materials for each software application in scope.[3]

Once you identify and evaluate assets, your next step is to build a high-level model of how the systems communicate and interact with each other. You can do this by developing an ITS architecture, which includes a visual map of all logical and physical interconnections, data flows between field devices and central controls, and the specific communication protocols used across the network.

You must also comply with legislative or policy requirements unique to your jurisdiction, such as those relating to critical infrastructure or emergency management. You should review and understand this policy context so that requirements are not overlooked when you implement your action plans.

With a clear understanding of assets, architecture, and regulatory context, the working group can begin identifying vulnerable components. Before recording any vulnerabilities, it is important to determine how that data will be stored. For example, documentation of all vulnerable systems within a transport network is extremely sensitive and should have restricted viewership.

Once protection mechanisms are in place, you can start looking for vulnerabilities. This work is best done with help from information sharing groups and using threat intelligence resources, such as the CCCS resources shared at the end of this document.

To make the best use of open-source intelligence, asset registers should be in a format that can be used to query vulnerability databases such as the Common Vulnerabilities and Exposures database. A software bill of materials can also be used to search for inherited vulnerabilities in the supply chain.

As organizations complete the orient phase, they should also consider adopting standardized frameworks for risk assessment. For example, NIST SP 800-30 provides structured guidance for assessing likelihood and impact. Additional detail on risk assessment standards and frameworks is provided in Step 4.

Considerations for measuring value and criticality

Comparing value and criticality is an important part of identifying and documenting your environment. In the context of this guide, value and criticality are used to help organizations prioritize ITS assets, systems, and data.

Value refers to the relative importance of an asset based on the consequences of its compromise, including potential safety impacts, financial costs, service disruption, legal or regulatory implications, and reputational harm.

Criticality reflects how essential an asset is to maintaining safe and continuous operations, particularly the degree to which its loss, degradation, or manipulation would affect core transportation services or public safety. Consider rating or ranking criticality based on factors like:

- up-time requirements
- public facing visibility
- applicable laws, policies, standards, regulations, and guidelines
- degree of restoration required to achieve desired level of continuity
- sensitivity of data (for example: personally identifiable information)
- availability of fallback asset, manual overrides, or other redundancies

[3] The CCCS defines a software bill of materials as "a formal record of the details of various components used in building software as well as their supply chain relationships" and has released guidance on a shared vision of software bill of materials for cyber security in conjunction with international partners.

- dependency to other information system components

Table 1: Types of threats and scenarios
Understand the threat landscape helps you identify potential vulnerabilities and risks. Below are some common examples of types of cyber threat actors, and common attack vectors you may encounter.

Type of threat	Level of sophistication	Motivation
Nation state or state sponsored	High	Geo-political interests
Cyber criminals	Moderate	Financial gain
Hacktivists, terrorist groups, and thrill seekers	Low	Disruption, inflicting reputational damage, could be driven by ideology
Internal threats	Low. Internal threats do not commonly use sophisticated tools or techniques but are dangerous due to their privileged access and/or insider knowledge.	Grudge against the organization

Common attack vectors (types of attacks):
- network intrusion
- zero-day vulnerabilities
- malware
- denial of service (DoS)
- distributed denial of service (DDoS)
- social engineering
- phishing
- spear phishing
- side-channel attacks

Step 3: Create a current profile

After defining the cyber landscape, you need to assess and understand your organization's current position and capabilities.

This is accomplished by using a standardized assessment and evaluation framework or tool to measure the maturity across your organization. Many frameworks from reputable cyber security authorities exist to provide a common language for standards and controls.

Transport Canada's **ITS Cyber Security Self-Assessment Tool** is one tool you can use to assess your cyber posture. It includes a questionnaire that follows each of the NIST functions and establishes a maturity level according to the Capability Maturity Model Integration (CMMI) Scale. The tool explores several facets of security engineering, including culture, management, processes, and controls.

Summary of step 3: Create a current profile

- Choose your framework
- Make sure you have buy-in and customize framework as needed
- Measure current state

All relevant branches or teams should agree on the framework being used and participate in establishing the current state profile. Include OT teams to make sure that OT is represented in the assessment.

Once you have chosen a framework, avoid frequent changes to its setup. In some cases, modifying or adapting an existing assessment framework could enable more effective measurement or be more applicable for key internal stakeholders, but try to avoid making major changes to an established industry standard framework. Additionally, using an industry standard framework will make it easy for you to compare your results against similar organizations, but be wary of comparisons with organizations that use different or custom assessment frameworks.

Using Transport Canada's ITS Cyber Security Self-Assessment Tool

The purpose of the Cyber Security Self-Assessment Tool is to give you a way to obtain a "snapshot" of your organization's cyber maturity. This self-assessment will help you understand your current state profile and overall cyber security posture in 6 functions, 22 categories and 106 subcategories, aligning with the NIST Cyber Security Framework.

Full instructions for using the tool are available through the link above. You can also adjust the tool based on unique the requirements of your organization, as needed.

Understanding the Capability Maturity Model Integration Scale

The Cyber Security Self-Assessment Tool measures your organization's maturity score using levels that are based on the CMMI Scale. The scale is a 1-5 maturity scale (1 being the lowest and 5 being the highest). Maturity levels are defined below.

1. **Initial**

Processes at this level are usually undocumented and in a state of flux. They tend to be driven in an as needed, uncontrolled and reactive way.

Organizations within this level typically acknowledge security risks, have limited awareness of security risks at organizational level and their risk management approach is inconsistent and relies on the security awareness of the employees.

2. **Repeatable**

Processes are repeatable, with consistent results. Process discipline is not rigorous.

Organizations within this level have documented security management processes, with no organizational-wide approach or policies defined.

3. **Defined**

Defined and documented standard processes are set and are subject to some degree of improvement over time.

Organizations within this level have organizational wide security policies in place, with a defined review cycle.

4. **Managed**

Using control and process metrics, management can effectively control the processes.

Organizations within this level have formally defined metrics for all security processes and controls. Metrics are reviewed to assess effectiveness of controls. Processes are integrated at an organizational level, in such a way that a change on one process will trigger a change on all dependent processes.

5. Optimized

The focus is on continuous improvement of process performance through technological changes or upgrades.

Organizations within this level perform causal analysis and resolution and continuously loops feedback to the processes. Automated metrics are reported upon to make informed risk decisions and are continually reviewed and enhanced to ensure efficiency.

Step 4: Do a risk assessment

This step focuses on building an accurate picture of your organization's cyber risk and is informed by the vulnerabilities you identified in Step 2 and your organization's current cyber position as assessed in Step 3.

Cyber risk assessments share many of the core concepts with other risk management practices. Risk is a combination of impact and likelihood.

- **Likelihood** describes the probability of the risk occurring.
- **Impact** is a measurable estimate of potential losses related to a risk. It can be tied to a range of factors, including population size impacted, types of traffic in the environment, and throughput of roads.

By exploring these dimensions of risk, your organization can filter out unlikely or minimal impact scenarios and prioritize risks that are potentially imminent and have the potential to cause significant harm to your organization.

To estimate these values, you should include representatives from all relevant business units and require access to reliable sources of threat intelligence. We provide some resources at the end of the document in the section "Additional resources from the CCCS".

Risk assessments include evaluating the likelihood and impact, mitigation strategies and individuals responsible for actions. These are captured in a risk register, which is a listing of all the risks and vulnerabilities your organization has identified.

Summary of step 4: Do a risk assessment

- Choose a risk assessment standard. Then implement it and use it
- Create a risk register template for all risks
- Define your organization's risk tolerance and risk appetite
- Integrate managing cyber risks into your enterprise risk management system
- Risk assessments are done on a continuous basis, and include evaluating the impact and likelihood of risks

Risk assessments are an essential part of an enterprise risk management (ERM) strategy, which is an integrated approach to managing all risks your organization may face. Verify if your organization already has a ERM strategy, and if so, how cyber risks can be integrated into the strategy.

Figure 2, going from top to bottom, illustrates how you can integrate managing cyber risks into your organization's ERM strategy. NIST IR 8286 Integrating Cyber Security and Enterprise Risk Management offers more guidance in this process.

As you work on this strategy, your organization will define its risk tolerance, which would then inform cyber risk assessments.

ⓘ The ITS Cyber Security Self-Assessment tool includes a questionnaire to help you determine your organization's risk tolerance. A lower target profile indicates a higher risk tolerance, and a higher target profile indicates a lower risk tolerance level.

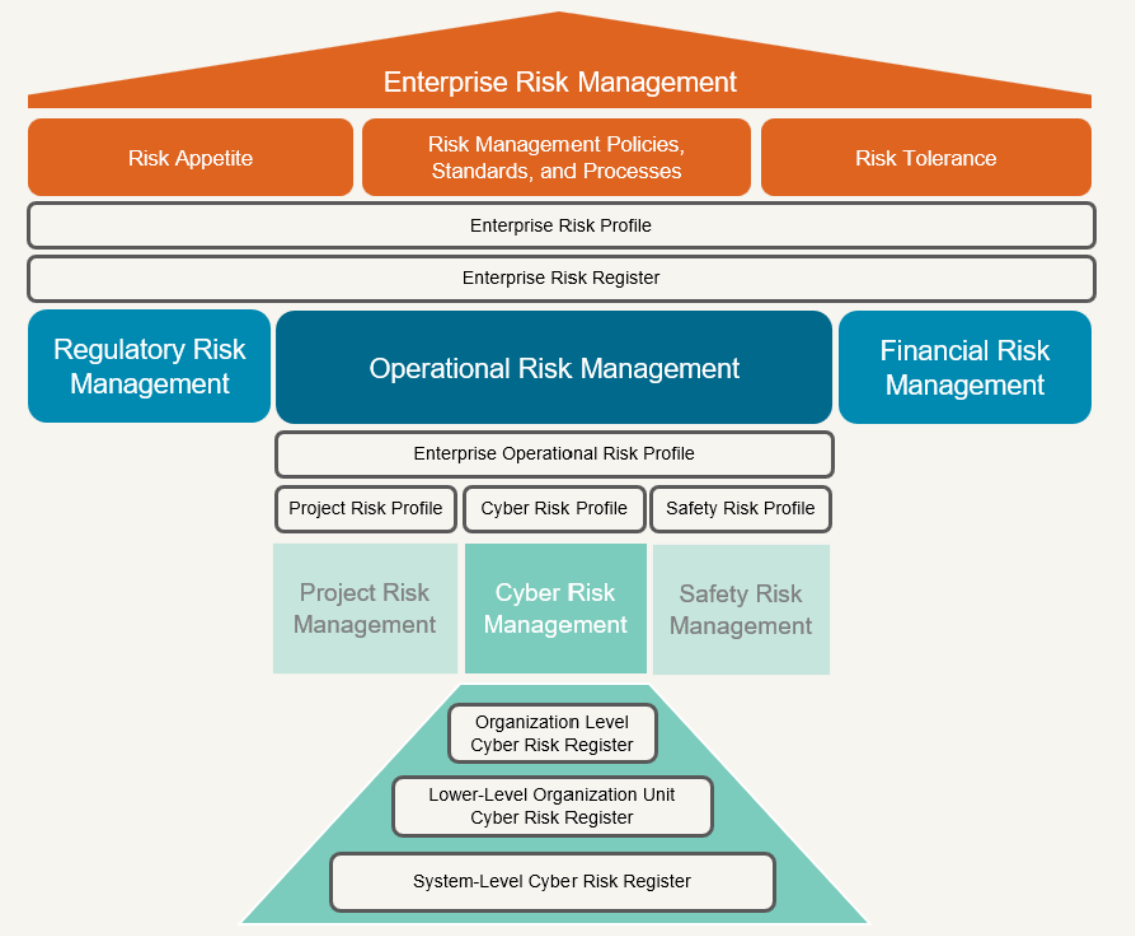
See Step 5 for more information on the Target Profile Assessment.

You should choose an established risk assessment standard (such as NIST SP 800-30 or Harmonized Threat and Risk Assessment Methodology (HTRA)) to ensure that the risk assessment process has a high degree of integrity.

Lastly, risk assessments should be embedded into your organization's culture and undertaken regularly, such as once or twice a year, as systems improve and the operating environment changes.

Your first few assessments should have a broad scope. As you begin to understand the risks better, you can do more specific assessments through risk registers created at more granular levels.

Figure 2: Example of integrating cyber security into managing enterprise risks



More guidance on managing OT risks

Network management is a critical control for the security of operational systems, which may be undertaken by a different team that manages the IT and OT assets.

Making sure that the IT and OT networks are segmented with controlled and instrumented interfaces is the bare minimum level of protection. It's also important that the individuals that manage the network are aware of the requirements of both interfaces.

The propagation of malware or cyber attacks between OT and IT (and vice versa) is a serious risk that you need to address. Malicious software could arrive via direct network interface, portable media, or remote access.

When managing interfaces between OT and IT networks, organizations typically apply one of two broad conceptual approaches to determine how trust, segmentation, and security controls are applied.

1. **Strict separation (zero-trust approach).** This approach treats all external or interconnected networks as untrusted by default. Strong segmentation and tightly controlled interfaces are used to minimize the risk of malware or unauthorized access moving between networks. This can be effective for protecting sensitive OT environments, but may require additional resources and can limit operational flexibility if not carefully designed.

2. **Risk-informed segmentation (proportional controls).** This approach applies security controls based on an assessment of relative risk between networks. Controls are tailored according to factors such as system criticality, exposure, and existing protections, enabling organizations to balance security with operational efficiency. While more flexible, this approach relies on accurate risk assessment and ongoing monitoring, and may be less effective if risks are underestimated.

Step 5: Create a target profile

Summary of step 5: Create a target profile

- Create a target profile based on relevant factors and the latest information

If you have a solid understanding of your organization's current risk profile, you can determine your organization's target profile (in other words, the desired state of your organization for it to be in a strong position to manage its risks).

The target profile will help you identify the gaps between your current state and your target state, and help you create viable action plans.

The ITS Cyber Security Self-Assessment Tool includes a target profile assessment that will help you define your desired state based on your organization's security needs.

This tool will give you a starting point, but further customization at the category or even subcategory level can be considered by experts within the organization.

Maximizing scores across all areas of the tool isn't realistic for most organizations. In the context of the CMMI scale used in the self-assessment tool, a score of 5 in any capability is highly difficult to achieve, and even the most mature organizations would struggle to reach and maintain it, so it would be wise to determine realistic goals. Additionally, a high score in a single area with low scores in other areas may imply that you've over-committed to a specific area and may need focus on other areas.

Finally, you should set your starting targets using the same scale as the current state profile from Step 3, like the CMMI scale used in the Cyber Security Self-Assessment Tool.

ⓘ The ITS Cyber Security Self-Assessment Tool allows you to manually modify your target profile for each sub-category. You can set target maturity levels from 2 to 5.

For sub-categories with current scores below level 3, we recommend setting level 3 as a minimum target level. Step 6 provides more guidance on going from a level 1 to a level 3.

Determining your target profile

The ITS Cyber Security Self-Assessment Tool will help you set both your current and target profile. Then, you'll compare these two states to see where your organization has the largest potential gaps.

The target profile assessment asks a series of questions that will help you set a target state based on the size of your organization, the community you serve, and what type of technology you have in service.

The assessment considers factors like:

- number of people within your jurisdiction
- kilometres of roads and pathways in your jurisdiction
- throughput of traffic in your jurisdiction
- awareness of regulatory requirements
- percentage of IT budget spent on cyber security
- number of full-time employees dedicated to cyber security in your organization
- recent cyber attacks experienced
- ITS technologies currently in use
- ITS technologies planned for implementation in the next 5 years
- amount of equipment your organization manages
- business goal
- desired security outcomes
- ideal risk tolerance
- understanding of the current threat landscape
- existence of an overall cyber risk strategy in your organization
- vendor management policies

Once you set an initial target state, you can adjust it over time. You can do this by:

- moving every subcategory's score up or down by 0.5 point increments
    - If you feel that the profile suggests a lower or higher target across the board, you can use this to quickly increase or decrease the target state scores
    - A target profile of a 3.5 or 4.5 will increase the target scores for all subcategories in the Identity and Protect functions (to a 4 or 5 respectively) and leave the others at 3 or 4
- manually adjusting your score
    - If you want complete control of your target profile, you can manually set scores for subcategories

Step 6: Determine, analyze, and prioritize gaps

The difference between your organization's target profile and current profile will help you identify gaps in processes, policies, and controls.

The CMMI scale provides a quantitative measure of these gaps, and the ITS Cyber Security Self-Assessment Tool recommends controls that can help close the gaps. Make sure to take slow, incremental steps towards your target state.

Summary of step 6: Determine, analyze, and prioritize gaps

- Analyze gaps according to estimated likelihood and impact
- Do a cost-benefit analysis to prioritize gaps

For example, if your organization is at a level 1 on a question, and your target state is a level 3 for those controls, do not be afraid of making small, gradual improvements that would increase your maturity to a level 2 for some time. Attempting to make large jumps in maturity can be difficult to plan and execute and may lead to delays and cost increases.

The tool highlights the relative size of the gaps for different capabilities, which can help your organization prioritize work. The Tool and Appendix A of the ITS Cyber Security Self-Assessment

Tool User Guide include recommendations for controls, but choosing which controls to implement will require you to evaluate your organization's goals, risks, and resources. A cost-benefit analysis (illustrated in the following section) can help to identify the activities that have the highest impact for the level of investment available.

Following a cost-benefit analysis, you may have to make optimization decisions. Some improvements may cost more than your available budget, and you need to take care to ensure that funding these activities does not come at the cost of an organization's ability to maintain its risk position.

In these cases, smaller projects may be better as they carry less project risk. The cyber security working group should work with financial and management stakeholders to create a plan that aligns with your organization's comfort level with cyber security and financial risks.

Larger projects should be assigned a combination of KPIs and milestones so that the working group can monitor how the plan is implemented in Step 7.

Cost-benefit analysis

There are many ways to do a cost-benefit analysis. Two are highlighted below: a simple finance-based method and a more complex risk-based method.

Both will need you to calculate the cost of implementing your plan, which can include:

- the initial cost of implementation
- maintenance costs over a set period
- cost of lost productivity or resources, and
- cost of determining feasibility

When calculating maintenance costs, the relevant period should be consistent with how likelihood is calculated. So, if a risk is likely to occur within the next 6 years, the scope of the maintenance costs would be 6 years.

When determining the cost of lost productivity or resources, make sure that all stakeholders are consulted to ensure unintended impacts are not overlooked.

Finance-based method

A finance-based analysis evaluates risks based on estimated financial impact before and after implementation. Each process, policy or control would typically fit into one of the subcategories from Appendix A of the ITS Cyber Security Self-Assessment Tool User Guide.

A low cost/benefit ratio indicates a higher relative impact, meaning that you should prioritize the item, while a high cost/benefit ratio indicates that the costs of implementation are high compared to the possible value.

Table 2: Example of cost-benefit analysis using a finance-based method

Process, policy, or control	Financial impact of current risk	Estimated financial impact after implementation	Risk delta [1]	Cost to implement	Cost / benefit ratio [2]
Control A	$100,000	$20,000	$80,000	$200,000	2.5

[1] Risk delta = Financial impact of current risk - Estimated financial impact after implementation

[2] Cost/Benefit ratio = Cost to implement / Risk delta

Risk-based method

This method considers various risk-based factors, including both likelihood and impact. You will need to use a matrix or framework to make sure your analysis is consistent, such as the Assessment Scale in NIST SP 800-30 (summarized in table 4.7.2).

Table 3: Example assessment scale

Risk level	Score	Description
Very high	10	**Very high risk** means that a threat event could be expected to have **multiple severe or catastrophic** adverse effects on organization operations, organizational assets, individuals, other organizations, or the nation
High	8	**High risk** means that a threat event could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, individuals, other organizations, or the nation
Moderate	5	**Moderate risk** means that a threat event could be expected to have a **serious** adverse effect of organizational operations, organizational assets, individuals, other organizations, or the nation
Low	2	**Low risk** means that a threat event could be expected to have a **limited** adverse effect on organizational operations, organizational assets, individuals, other organizations, or the nation
Very low	0	**Very low risk** means that a threat event could be expected to have a **negligible** adverse effect on organizational operations, organizational assets, individuals, other organizations, or the nation

Alternatively, your organization can create its own matrix. Table 4 illustrates how a cost-benefit analysis can be performed using the assessment scale in Table 3.

Table 4: Example of cost-benefit analysis using a risk-based method

Process, policy, or control	Current risk	Estimated risk after implementation	Risk delta [1]	Cost to implement	Cost / benefit ratio [2]
Control A	High (8)	Low (2)	6	$200,000	33,333.33

[1] Risk delta = Current risk - Estimated risk after implementation

[2] Cost/Benefit ratio = Cost to implement / Risk delta

Implementing a control would be based on the relative size of the cost/benefit ratio among all controls. In some cases, addressing a risk might be too expensive. In this situation, your organization should reduce the risk as low as reasonably practicable, meaning the harm of a potential risk should be reduced as much as possible, given organizational constraints.

Step 7: Implement your action plan

Implementing your action plan may involve both small and large investments, projects, and resource commitments.

To start implementing your action plan, it is important to get executive support and determine a budget before carrying out the identified action, control, or risk treatment. This can be a challenging process. Below are some methods that can support you in obtaining executive support.

- **Develop a business case:** summarize risks and benefits, using your results from Step 6, and emphasize the return on investment. The contents can be developed into a business case document.
- **Link to organizational goals:** frame cyber security as a business enabler, not just a technical issue, by showing how cyber security supports safety, reliability, compliance, and reputation.
- **Leverage external standards:** reference CCCS and NIST frameworks to strengthen credibility.
- **Phase funding requests:** start with smaller projects tied to achievable milestones to build momentum and trust.

Summary of step 7: Implement your action plan

- Identify, approve and implement action plans
- Monitor action plans and associated risks over time using KPIs and milestones
- Assign delivering action plan to sector with appropriate experts

For all action plans, you need to continue to monitor work to make sure implementation is sustained and outcomes are being met on an ongoing basis.

The cyber security working group should work with your organization's management to oversee the delivery of the action plan but should also delegate specific activities to sector experts where appropriate.

For example, the work of delivering an OT program may be monitored by the cyber security working group through KPIs and milestone tracking, but specialist OT engineers may be required to perform the actual work.

Work should consider confidentiality, integrity, and availability requirements of systems and data at all stages. For example, any "down time" required to make changes should be balanced against the availability impact of the cyber attack against which it is defending.

When implementing action plans, progress towards maturing the organization's cyber security posture may be monitored by regularly updating the current profile and subsequently comparing it to the target profile. You can reuse the ITS Cyber Security Self-Assessment Tool for this exercise.

Continual improvement after reaching target state

Cyber security is a moving target. Threats and vulnerabilities evolve constantly and require organizations to adapt and react in an equally dynamic way. Achieving your target state should not be your "finish line"; it's the foundation for ongoing improvement. Sustaining progress will demand continued investment, executive commitment, and a culture that treats cyber security as a core business priority.

Regular reviews and updates are essential, but the frequency should align with your organization's resources and risk profile. Improvement does not need to be linear; what matters is maintaining momentum and embedding cyber security into everyday decision-making. Celebrate milestones and regular communication progress can help keep stakeholders engaged and motivated.

Following the steps in this guide will keep your understanding of threats, risks, and vulnerabilities up to date, informing future planning and action. Success depends on accurate, timely data and collaboration, leveraging vulnerability databases, threat intelligence, and information sharing from peer organizations.

For trusted guidance and alerts, the Canadian Centre for Cyber Security (CCCS) is a key resource. CCCS provides advice, services, and threat notifications to help organizations strengthen resilience. See the resource table at the end of this document for examples of CCCS tools and publications.

Additional resources from the CCCS

Alerts and advisories

The CCCS issues alerts and advisories on potential, imminent or actual cyber threats, vulnerabilities or incidents affecting Canada's critical infrastructure.

https://cyber.gc.ca/en/alerts-advisories

Report a cyber incident

Reporting a cyber incident helps the CCCS keep Canada and Canadians safe online. Your information will enable the CCCS to provide cyber security advice, guidance, and services. Reporting to the CCCS will not launch an immediate law enforcement response, such as investigating cybercrime or other criminal offences.

https://cyber.gc.ca/en/incident-management

Publications

These guidance documents include recommendations and actions that your organization can implement to protect your networks, systems, and information.

https://www.cyber.gc.ca/en/guidance

Assemblyline – Malware detection and analysis

This service allows partners to disclose and exchange malware samples with the CCCS. The service allows for timely and automated results that an organization can integrate within their internal cyber triage processes

https://www.cyber.gc.ca/en/tools-services/assemblyline

National Cyber Threat Notification System

This system notifies Canadian organizations of misconfigured services, vulnerabilities, and compromised infrastructure on their IP space. Notifications are based on data received from trusted open source and commercial threat feeds and the CCCS.

https://www.cyber.gc.ca/en/guidance/national-cyber-threat-assessment-2025-2026

Transportation sector partnerships team

To join the CCCS's transportation sector partnerships team distribution list, please email: transport-par@cyber.gc.ca.

If you're interested in learning more about advanced services from the CCCS get in touch by emailing contact@cyber.gc.ca.