# ÉTABLIR UN PROGRAMME DE CYBERSÉCURITÉ INTÉGRÉE : GUIDE À L'INTENTION DES PROPRIÉTAIRES/EXPLOITANTS D'INFRASTRUCTURES ROUTIÈRES CANADIENNES ET DES PROFESSIONNELS DES STI

2026

Transports Canada Transport Canada

Canada

Ce guide aide les autorités routières et les propriétaires et les exploitants d'infrastructures à élaborer et à faire évoluer un programme de cybersécurité des STI.

Aussi disponible en anglais sous le titre : « Establishing an Enterprise Cyber Security Program: A Guide for Canadian Road Infrastructure Owners/Operators and ITS Professionals »



TP 15628F

Cat. T89-24/2025F-PDF

ISBN 978-0-660-75823-7

# Table des matières

# Acronymes et abréviations

Vous trouverez ci-dessous une liste des acronymes utilisés dans ce guide. Chaque terme est épelé en entier la première fois qu'il apparaît dans le texte principal, suivi de son acronyme pour les utilisations ultérieures.

CCC – Centre canadien pour la cybersécurité

CMMI – Intégration du modèle de maturité des capacités

DDoS – déni de service distribué

DoS – déni de service

GRE – gestion des risques d'entreprise

IdO – Internet des objets

IRC – indicateur de rendement clé

LPRPDE – Loi sur la protection des renseignements personnels et les documents électroniques

NIST – Institut national des normes et de la technologie

SGT – système de gestion du trafic

STI – systèmes de transport intelligents

TI – technologie de l'information

TO – technologie opérationnelle

# Résumé

Les systèmes de transport intelligents (STI) transforment le transport routier en améliorant la sécurité, l'efficacité et la mobilité grâce à une connectivité accrue, à l'automatisation et à l'échange de données. Parallèlement, cette dépendance croissante aux technologies numériques a élargi le champ des cybermenaces, exposant les infrastructures de transport à des risques pouvant compromettre la sécurité publique, perturber les opérations, nuire à la réputation des organisations ou entraîner des pertes financières. Par conséquent, la cybersécurité est maintenant un élément essentiel de systèmes de transport résilients et fiables.

Ce guide aide les propriétaires et les exploitants d'infrastructures routières canadiennes dans leurs efforts pour établir, renforcer ou maintenir un programme de cybersécurité pour leurs STI. Il fournit des conseils pratiques et détaillés pour la gestion des cyberrisques dans des environnements où les technologies de l'information (TI), les technologies opérationnelles (TO) et les systèmes critiques pour la sécurité convergent de plus en plus, et s'articule autour d'un processus structuré en sept étapes pour la création ou l'amélioration d'un programme de cybersécurité. Ces conseils sont conformes au Cadre d'amélioration de la cybersécurité des infrastructures critiques de l'Institut national des normes et de la technologie (NIST) et privilégient une approche axée sur les risques et la maturité.

Ce document n'est ni exhaustif ni prescriptif. Il vise plutôt à compléter les normes et les orientations existantes d'autorités reconnues, notamment Sécurité publique Canada et le Centre canadien pour la cybersécurité (CCC). En appliquant les principes et les étapes décrits dans ce guide, les organisations peuvent renforcer la résilience de leurs STI, mieux protéger la sécurité publique et les données, et favoriser le déploiement sécuritaire des technologies de transport actuelles et futures.

# Introduction : Sécuriser un paysage de cybermenaces en constante évolution et portée de ce guide

Les technologies de transport routier évoluent rapidement, améliorant la sécurité, la mobilité et l'efficacité pour tous les usagers. Cependant, ces progrès peuvent aussi engendrer de nouveaux risques en matière de cybersécurité. Auparavant, les mesures de protection en matière de cybersécurité étaient principalement concentrée sur l'isolation des réseaux et la création d'un périmètre de sécurité strict afin d'empêcher les menaces de pénétrer les défenses d'une organisation. Bien que cette approche demeure importante, la cybersécurité exige désormais des organisations qu'elles développent de nouvelles méthodes pour prévenir un éventail plus large de menaces de plus en plus sophistiquées, y répondre et s'en remettre. Face à l'expansion du paysage des cybermenaces, la sécurisation des systèmes de transport intelligents (STI) devient une priorité de plus en plus importante.

Ce guide vise à aider les autorités routières et les propriétaires et les exploitants d'infrastructures routières à développer et à perfectionner un programme de cybersécurité pour leurs STI. Il fournit des conseils sur :

- la mise en place d'un tel programme
- l'élaboration d'un plan pour l'amélioration de la posture de cybersécurité de votre organisation
- les contrôles courants que votre organisation peut mettre en œuvre.

Il est conçu pour être conforme au cadre de l'Institut national des normes et de la technologie (NIST) (en anglais) pour l'amélioration de la cybersécurité des infrastructures critiques.

Comme l'illustre la figure 1 (ci-dessous), la mise en place du programme comprend sept étapes réparties en quatre phases distinctes. La section « Comment créer ou améliorer un programme de cybersécurité » suit directement cette séquence afin de faciliter la mise en œuvre. Puisque le maintien de la résilience exige un engagement continu, ces étapes sont conçues pour être itératives, permettant ainsi à votre organisation d'améliorer continuellement sa posture de sécurité au fil du temps.

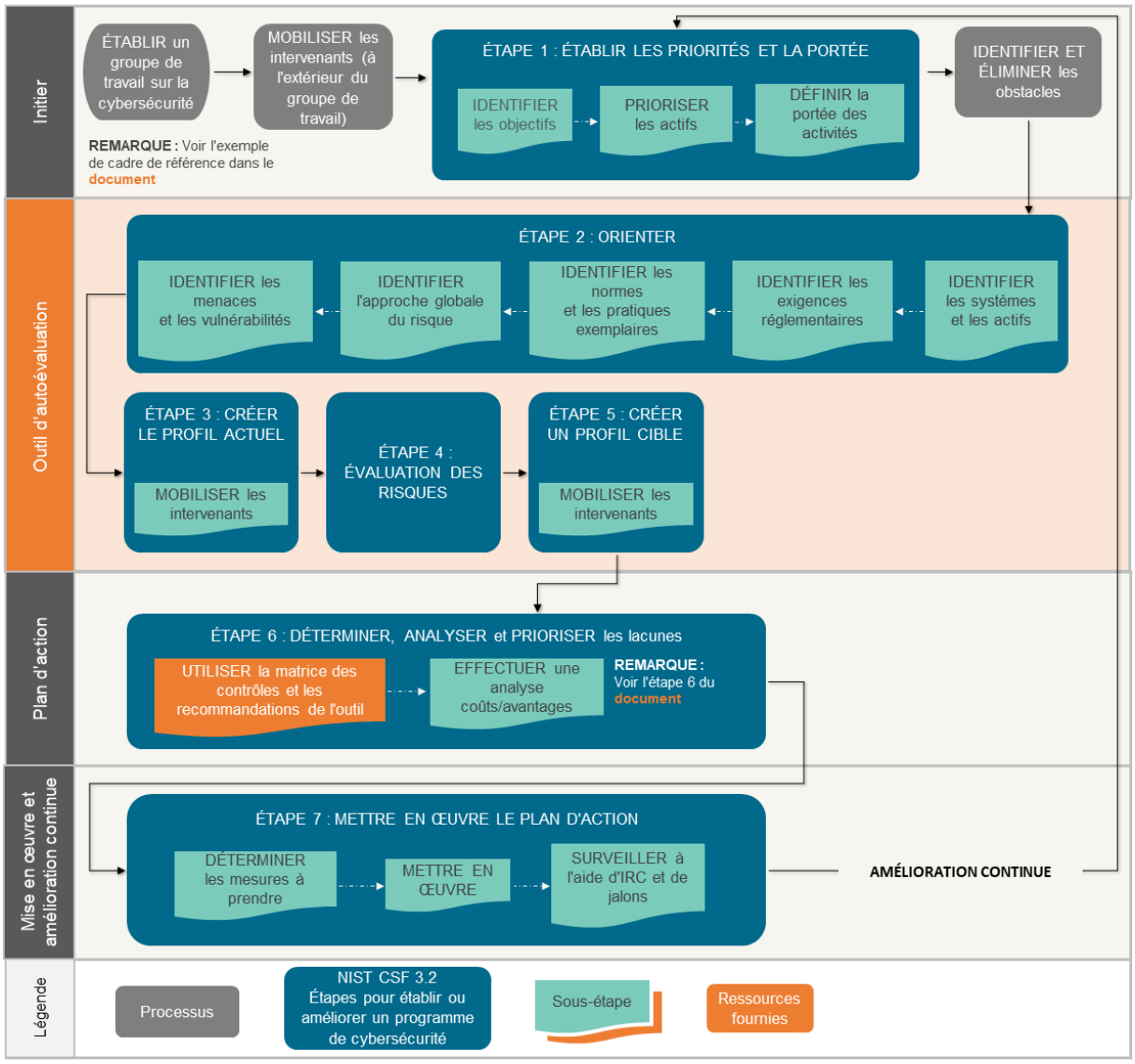
Bien que ce document serve de guide de base, il devrait être utilisé en complément des pratiques exemplaires les plus récentes de Sécurité publique Canada, du Centre canadien pour la cybersécurité (CCC) et des organismes de réglementation internationaux reconnus.

Ce guide complète les autres ressources disponibles sur la page Web de Transports Canada consacrée à la cybersécurité des infrastructures routières, notamment :

- **Document d'Information de cybersécurité des STI :** Un document d'information de haut niveau destiné aux dirigeants d'infrastructures routières sur l'importance d'investir dans la résilience en matière de cybersécurité.
- **FAQ sur la cybersécurité des STI :** Une page Web de questions fréquentes répondant aux questions courantes sur la gestion des cyberrisques et le renforcement de la cyberrésilience des STI.
- **Outil d'autoévaluation de la cybersécurité des STI :** Un outil sous forme de tableur comprenant un questionnaire d'évaluation du profil actuel et un questionnaire d'évaluation du profil cible, qui peut être utilisé pour générer des recommandations et des actions visant à améliorer la posture cybernétique de votre organisation. L'outil est accompagné d'un guide d'utilisation. Vous devez fournir une adresse courriel pour télécharger l'outil et le guide d'utilisation.

- Introduction à la cybersécurité des technologies opérationnelles des infrastructures routières : Ce document fournit des conseils de base et des pratiques exemplaires pour vous aider à concevoir et à mettre en œuvre un programme de cybersécurité.

Figure 1: Aperçu des étapes à suivre pour créer ou améliorer un programme de cybersécurité




# Défis de cybersécurité dans les environnements STI connectés et convergents

Le paysage actuel des systèmes de gestion du trafic (SGT) est étroitement interconnecté pour permettre une gestion efficace et sécuritaire des ressources de transport. Les systèmes de transport

intelligents (STI) sont une intégration de l'infrastructure de transport routier, des véhicules et des communications.

Un sous-produit de cette interconnexion peut être le brouillage des frontières entre les environnements de technologie de l'information (TO) traditionnellement isolés et de technologie opérationnelle (TI) hautement connectés. C'est ce qu'on appelle la convergence et, sans mesures proactives, vous pouvez exposer votre STI à de nouvelles vulnérabilités et à un paysage de menaces plus large.

Un SGT traditionnel comprend plusieurs composantes, telles que des contrôleurs de signal, des capteurs de circulation, des télévisions en circuit fermé et des panneaux à messages variables. De nombreux composants anciens et existants d'un SGT n'étaient généralement pas destinés à être connectés à des réseaux externes. Par conséquent, les contrôles de sécurité normalisés communs aux systèmes de TI, comme l'authentification et l'autorisation obligatoires, n'ont pas été priorisés lors de leur développement. L'absence de contrôles de sécurité de base pose un risque potentiel lors de l'intégration d'une infrastructure SGT existante avec un système STI moderne. Étant donné que des STI introduit une connectivité externe à des dispositifs auparavant isolés du réseau, il est essentiel de comprendre l'architecture SGT existante et d'identifier les failles de sécurité potentielles afin de réduire l'exposition aux risques avant l'intégration.

Un autre défi que les exploitants de STI doivent relever est l'interopérabilité. De nombreux environnements d'infrastructure sont constitués d'anciens et de nouveaux systèmes ou plateformes qui coexistent et interagissent. Les solutions de connectivité et les intégrations personnalisées sont courantes dans ces environnements et peuvent être difficiles à sécuriser avec les derniers correctifs de sécurité, si ceux-ci sont disponibles, en particulier lorsque les systèmes existants ne bénéficient pas du soutien du fournisseur ou lorsque l'application de mises à jour risque de perturber les systèmes opérationnels intégrés.

De plus, un SGT recueille et envoie de grandes quantités de données à divers terminaux et via des appareils connectés. Ces données sont ce qui permet au SGT de fonctionner correctement, efficacement et en toute sécurité. Les terminaux qui envoient et reçoivent des données dans un SGT sont souvent des appareils de l'Internet des objets (IdO) avec une exposition inhérente à Internet. Ces appareils de l'IdO pourraient ne pas être suffisamment renforcés avant le déploiement. Par conséquent, les données ou l'intégrité opérationnelle de ces composants peuvent être compromises ou manipulées.

# Principaux risques en matière de cybersécurité

**Sécurité -** Les cybermenaces ciblant les feux de circulation, les systèmes de surveillance ou les infrastructures d'intervention d'urgence, comme le 9-1-1 et les systèmes de détection d'incidents, pourraient poser de graves risques pour la sécurité des navetteurs et des exploitants routiers.

L'infrastructure de transport devrait être développée avec des mesures accrues pour assurer la sécurité des usagers, des navetteurs et des travailleurs. Si les systèmes de sécurité et leurs dispositifs de sécurité étaient compromis, les usagers, les navetteurs et les conducteurs pourraient être exposés à des blessures ou à la mort. Étant donné que les systèmes de sécurité sont des cibles qui fournissent un levier important aux attaquants, ils doivent être parfaitement protégés.

**Perturbation opérationnelle -** Les cyberattaques peuvent entraîner des ralentissements de la circulation, des arrêts et de la congestion, affectant l'efficacité des réseaux de transport et perturbant les chaînes d'approvisionnement. Par exemple, une attaque ciblée pourrait entraîner la paralysie d'un système de régulation de la circulation, ce qui engendrerait une augmentation de la congestion routière, un risque accru d'accidents et des perturbations sur les principaux axes de transport.

Une attaque peut entraîner la perturbation du SGT, entraînant des ralentissements de la circulation, des fermetures ou des embouteillages. Selon la cible et la gravité de l'attaque, les conséquences pourraient avoir un impact sur d'autres secteurs d'infrastructures essentiels, les chaînes

d'approvisionnement et une meilleure santé économique. Par exemple, une attaque ciblée pourrait entraîner la perte de fonctionnement d'un système de contrôle de voie, ce qui entraînerait une augmentation de la congestion, un risque d'accidents de la route et des perturbations des principales voies de transport.

**Atteinte à la réputation -** Une atteinte ou une perturbation sécuritaire importante pourrait nuire à la réputation de l'organisation touchée et réduire l'appui du public aux technologies de transport connecté en général.

Dans les situations où il y a atteinte à la protection des données contenant des renseignements personnels, tels que des noms, des adresses ou d'autres renseignements sensibles, il peut y avoir des risques importants pour la vie privée du public (par exemple, fraude et vol d'identité), et une atteinte à la réputation de l'organisation. Les renseignements personnels doivent être protégés de manière appropriée et votre organisation doit comprendre les exigences législatives applicables en matière de traitement des données, telles que la Loi sur la protection des renseignements personnels et les documents électroniques (LPRPDE), la Loi sur la protection des renseignements personnels et/ou toute loi provinciale pertinente en matière de protection de la vie privée ou exigences organisationnelles .

**Conséquences financières** - Les attaques par rançongiciel, les amendes réglementaires et les responsabilités juridiques peuvent entraîner des pertes financières importantes.

Cela peut prendre de nombreuses formes, qu'il s'agisse de payer la valeur d'extorsion demandée par un attaquant (rançongiciel), de frais juridiques, atteinte à la réputation ou dommages aux infrastructures.

# Comment créer ou améliorer un programme de cybersécurité

L'élaboration d'un programme de cybersécurité prendra du temps, des efforts et des ressources. Cela peut s'avérer difficile, car les personnes et les experts en la matière ont également d'autres responsabilités au sein de l'organisation. Cependant, les avantages d'un programme de cybersécurité bien élaboré l'emportent sur le coût. Il est important que les personnes qui élaborent le programme de cybersécurité aient le temps et le soutien de la direction nécessaires pour le faire – cela ne devrait pas devenir une initiative peu prioritaire. La FAQ sur la cybersécurité sur notre page Web répond également à certaines questions courantes concernant les considérations pour les propriétaires et les exploitants d'infrastructures routières plus petits ou plus limités en ressources.

Avant de lancer un programme de cybersécurité, vous devriez mettre sur pied un groupe de **travail sur la cybersécurité** décrit ci-dessous. Une fois ce groupe de travail en place, nous présenterons sept (7) étapes pour élaborer un programme de cybersécurité. Veuillez noter que dans le texte de ces étapes, lorsque nous faisons référence à « vous », nous faisons référence au groupe de travail.

# Mettre sur pied un groupe de travail sur la cybersécurité comme base d'un programme de cybersécurité

Un **groupe de travail spécialisé en cybersécurité** peut promouvoir une approche coordonnée de la cybersécurité au sein de toute l'organisation.

Ce groupe de travail doit être créé pour mener (ou commencer) les tâches, prendre des décisions et superviser le processus.

Les responsabilités d'un groupe de travail sur la cybersécurité comprennent habituellement :

- l'approbation des cyberrisques acceptables
- l'approbation des fournisseurs tiers
- l'approbation du matériel de formation sur la cybersécurité
- la surveillance de la mise en œuvre de programmes ou des cyberinitiatives
- mesurer continuellement la cybermaturité de leur organisation

Un groupe de travail réussi comporte plusieurs éléments :

- le pouvoir (technique et opérationnel) de prendre des décisions liées à la portée et au mandat du groupe;
- la capacité d'obtenir du financement pour le travail du groupe;
- la représentation de tous les groupes d'intervenants internes touchés, y compris les TI, les TO et la sécurité, et représentation de plusieurs niveaux organisationnels, y compris la direction, la technique et la direction
- des réunions régulières qui déterminent, attribuent et suivent les actions;
- partager l'information avec l'ensemble de l'organisation au moyen de mises à jour régulières et de programmes de formation;

L'appui de la haute direction au groupe de travail sur la cybersécurité est un aspect essentiel. Il fournit au groupe une crédibilité, un accès aux ressources et une voie plus claire pour apporter les changements nécessaires.

L'annexe B du Guide de l'utilisateur de l'outil d'auto-évaluation de la cybersécurité des STI contient un exemple de cadre de référence pour un groupe de travail sur la cybersécurité qui comprend une approbation de la direction.

Une fois créé, le groupe de travail deviendra une force de *changement organisationnel*, en veillant à ce que la maturité de l'organisation en matière de cybersécurité soit mesurée, améliorée et maintenue au fil du temps.

Il existe de nombreux modèles reconnus de changement organisationnel, comme le modèle de Kotter.

## Huit activités pour diriger le changement[1] dans le cadre du groupe de travail sur la cybersécurité

### 1. Créez un sentiment d'urgence

Les organisations et leurs dirigeants doivent comprendre l'urgence des risques posés par les cyberattaques.

[1] Kotter, John P. *8 étapes pour accélérer le changement dans votre organisation*. 2018

Ce document présente un aperçu du paysage des cybermenaces au Canada et des risques potentielles liés à l'adoption de nouvelles technologies numériques.

**2. Bâtir une coalition d'orientation**

Un programme de cybersécurité réussi a de vastes répercussions sur les organisations, leurs employés et leurs processus. Il est important d'avoir du soutien et des conseils dans toute l'organisation.

Les intervenants qui ne font pas partie du groupe de travail peuvent être informés par les comptes rendus de réunion, de séances d'information et d'autres communications, comme des bulletins d'information et des formations, au besoin.

**3. Formez une vision stratégique**

L'identification de la vision stratégique du groupe devrait être l'une des premières tâches d'un groupe de travail. Une vision claire fournira une feuille de route pour les activités futures et une vue d'ensemble de ce que signifie le « succès ».

Cela est probablement éclairé par le mandat du groupe (voir l'annexe B du Guide de l'utilisateur de l'outil d'auto-évaluation de la cybersécurité des STI). Des conseils de niveau inférieur sur la façon de cerner les initiatives sont fournis dans les sections suivantes de la présente ligne directrice.

**4. Créez un réseau de champions de la sécurité**

La cybersécurité est un problème trop important pour être abordé par un seul groupe dédié. Pour être évolutif et efficace, il est essentiel de nommer des champions de la sécurité locaux, qui peuvent identifier et signaler les problèmes. Cela peut nécessiter des campagnes de formation et de sensibilisation. Dans la mesure du possible, recherchez des personnes ayant une expertise en cybersécurité pour se joindre au groupe de travail.

**5. Éliminez les obstacles**

Le groupe de travail devrait cerner et cibler les principaux obstacles à l'amélioration de la sécurité. Les obstacles varient d'une organisation à l'autre et peuvent inclure :

- des structures organisationnelle cloisonnées
- les pratiques de gestion des risques incomplètes ou inexistantes
- la manque de planification
- un financement limité
- une répartition diffuse des responsabilités

**6. Concentrez-vous sur les gains à court terme**

Les gains rapides sont un moyen efficace de motiver les groupes, de montrer des progrès et de la valeur.

De plus amples détails sur la détermination des mesures pour le groupe sont énumérés ci-dessous. Il est important que le groupe mesure et fasse la promotion des réussites auprès des parties prenantes.

**7. Continuez**

La cybersécurité est un domaine qui évolue rapidement et le maintien de votre posture de sécurité nécessite une concentration. Pour réaliser des progrès continus, le groupe devra se réunir régulièrement et s'assurer que les mesures sont réalisées, célébrées et promues auprès des intervenants.

**8. Restez agile**

Pour maintenir les progrès, vous devez être à l'aise avec les changements fréquents. Cela doit être intégré à la culture de votre organisation, mais les changements doivent toujours être liés à vos

objectifs organisationnels. Vous pouvez y parvenir en mesurant les résultats et en effectuant des études avant/après sur la maturité organisationnelle.

Notre outil d'auto-évaluation de la cybersécurité des STI peut appuyer ce travail.

## Pièges courants des groupes de travail sur la cybersécurité

### Manque d'objectifs clairs

La cybersécurité est un sujet intéressant dont les passionnés discuteront avec plaisir. Bien que cela puisse être excellent pour les premières réunions, il est essentiel que ces connaissances soient transformées en tâches.

Les ordres du jour des réunions des groupes de travail peuvent aider à assurer un équilibre entre la discussion informative et l'activité pendant les réunions.

### Fatigue

La participation aux réunions des groupes de travail peut commencer à diminuer, surtout s'il y a de longues périodes sans progrès visibles. Maintenir l'élan devrait être une tâche clé pour le président du groupe de travail.

L'établissement et le suivi des indicateurs de rendement clé (IRC), la discussion des progrès lors des réunions et la célébration des jalons peuvent aider à maintenir l'élan, tandis qu'un manque de financement ou de reconnaissance de la direction peut l'entraver.

La formation et la sensibilisation peuvent aider à s'assurer que les membres comprennent ce qui est en jeu. Des « moments de sécurité » réguliers qui explorent l'impact des défaillances en matière de cybersécurité sur d'autres entreprises peuvent aider à s'assurer que les membres comprennent l'importance des activités du groupe de travail.

### Ne pas établir de priorités

Lorsque des tâches sont assignées à des membres d'un groupe de travail, il est important de se rappeler que ces membres ont également d'autres tâches qui se disputent leur attention.

Pour éviter que les cybertâches ne soient oubliées, il est important de ne pas surcharger les membres du groupe. Pour vous aider à prioriser les tâches, chacune doit être liée aux objectifs ou aux risques de l'entreprise.

# Étape 1 : Établir l'ordre de priorité et définir la portée

Il est essentiel de déterminer vos principaux objectifs, tels que la fiabilité du système, l'intégrité des données et la sécurité publique, pour s'assurer que les protections de cybersécurité sont liées aux besoins réels.

Les objectifs généraux suivants sont suggérés comme point de départ, mais le groupe de travail sur la cybersécurité pourrait avoir des idées plus spécifiques qui pourraient être intégrées et complétées :

- protéger le personnel et les personnes qui utilisent le réseau de transport
- assurer la fiabilité du réseau de transport pour tous les usagers

**Résumé de l'étape 1 :**

- Déterminer les principaux objectifs opérationnels
- Définir la portée du programme de cybersécurité

Pour élaborer un programme de cybersécurité qui reflète ces objectifs, il est important de définir la portée des activités. Une portée bien définie vous donnera non seulement une idée des ressources dont vous aurez besoin, mais elle fournira également les limites du système à modéliser à des étapes ultérieures.

Voici quelques facteurs à considérer :

- **le stade ou la maturité du programme de cybersécurité** – par exemple : définition initiale des besoins, conception détaillée, développement, étapes finales de mise en œuvre, maintenance et amélioration
- **l'environnement de risque** – les actifs et services à risque, réseaux, etc.
- **l'objectif du programme** – les principales exigences de changement nécessiteront une évaluation détaillée de la portée, tandis que les exigences de haut niveau auront une portée plus large
- **les contraintes de coût et de temps** – des considérations pratiques peuvent limiter la portée[2]

La portée technique du programme de cybersécurité de votre organisation ne se limitera pas aux systèmes informatiques. Les TO, les systèmes de sécurité et les systèmes embarqués sont susceptibles d'être tout aussi importants pour les objectifs déclarés de l'organisation.

[2] Méthodologie d'évaluation harmonisée de la menace et des risques (EMR). (2007). MS-4

# Étape 2 : Orienter

La « phase d'orientation » permet de définir le contexte dans lequel le groupe de travail sur la cybersécurité évoluera. Il s'agit notamment d'identifier les actifs, les connexions, les interfaces et le cadre législatif, ainsi que de comprendre les vulnérabilités et les menaces.

**Résumé de l'étape 2 :**

- Identifier les actifs, les connexions et les interfaces
  - Créer un modèle de système d'information
- Comprendre le paysage législatif
- Identifier les vulnérabilités
  - Documenter les vulnérabilités sécurisées

Une activité fondamentale de cette phase consiste à dresser un inventaire complet des actifs concernés. À titre d'exemple, il peut s'agir d'un registre des actifs des composants des systèmes TO et TI. Vous pouvez utiliser la section « Gestion des actifs » du référentiel NIST (voir l'annexe A 1.2 du guide d'utilisation de l'outil d'auto-évaluation de la cybersécurité des STI) pour créer ce registre. En ce qui concerne les logiciels, vous pouvez créer une nomenclature logicielle pour chaque application concernée.[3]

Une fois les actifs identifiés et évalués, l'étape suivante consiste à élaborer un modèle de haut niveau décrivant la communication et l'interaction entre les systèmes. Pour ce faire, vous pouvez développer une architecture des STI, incluant une représentation visuelle de toutes les interconnexions logiques et physiques, des flux de données entre les dispositifs de terrain et les commandes centrales, ainsi que des protocoles de communication spécifiques utilisés sur le réseau.

Vous devez également respecter les exigences législatives et réglementaires propres à votre juridiction, notamment celles relatives aux infrastructures critiques ou à la gestion des urgences. Il est important d'examiner et de comprendre ce contexte réglementaire afin de ne négliger aucune exigence lors de la mise en œuvre de vos plans d'action.

Grâce à une compréhension claire des actifs, de l'architecture et du contexte réglementaire, le groupe de travail peut commencer à identifier les composantes vulnérables. Avant de consigner toute vulnérabilité, il est essentiel de déterminer le mode de stockage des données. Par exemple, la documentation relative à tous les systèmes vulnérables d'un réseau de transport est extrêmement sensible et son accès doit être restreint.

Une fois les mécanismes de protection en place, vous pouvez commencer la recherche de vulnérabilités. Ce travail est optimisé par le recours à des groupes de partage d'informations et à des ressources de veille sur les menaces, telles que les ressources CCC mentionnées à la fin de ce document.

Pour tirer pleinement parti des renseignements provenant de sources ouvertes, les registres d'actifs doivent être dans un format permettant d'interroger des bases de données de vulnérabilités telles que la base de données CVE (*Common Vulnerabilities and Exposures*). Une nomenclature logicielle peut également servir à rechercher les vulnérabilités héritées dans la chaîne d'approvisionnement.

[3] Le CCC définit une nomenclature logicielle comme « un enregistrement formel des détails des différents composants utilisés dans la construction de logiciels ainsi que de leurs relations avec la chaîne d'approvisionnement » et a publié des lignes directrices sur une vision partagée de la nomenclature logicielle pour la cybersécurité en collaboration avec des partenaires internationaux.

Une fois la phase d'orientation terminée, les organisations devraient envisager d'adopter des cadres normalisés pour l'évaluation des risques. Par exemple, la publication spéciale 800-30 du NIST fournit des recommandations structurées pour évaluer la probabilité et l'impact. Des renseignements supplémentaires sur les normes et les cadres d'évaluation des risques sont fournis à l'étape 4.

## Considérations pour mesurer la valeur et la criticité

La comparaison de la valeur et de la criticité est un élément important de l'identification et de la documentation de votre environnement. Dans le cadre de ce guide, les notions de valeur et de criticité sont utilisées pour aider les organisations à prioriser leurs actifs, systèmes et données STI.

La valeur désigne l'importance relative d'un actif en fonction des conséquences de sa compromission, notamment les impacts potentiels sur la sécurité, les coûts financiers, les interruptions de service, les implications juridiques ou réglementaires et l'atteinte à la réputation.

La criticité reflète le caractère essentiel d'un actif pour le maintien de la sécurité et de la continuité des opérations, en particulier la mesure dans laquelle sa perte, sa dégradation ou sa manipulation affecterait les services de transport essentiels ou la sécurité publique. Tenez compte de la criticité de la cotation ou du classement en fonction de facteurs tels que :

- les exigences en matière de temps de disponibilité
- la visibilité du public
- les lois, politiques, normes, règlements et lignes directrices applicables
- le degré de restauration requis pour atteindre le niveau de continuité souhaité
- la sensibilité des données (par exemple, les renseignements personnellement identifiables);
- la disponibilité d'actifs de secours, de remplacements manuels ou d'autres redondances
- la dépendance à l'égard d'autres composantes du système d'information

**Tableau 1 : Types de menaces et scénarios**

Comprendre le contexte des menaces vous aide à identifier les vulnérabilités et les risques potentiels. Vous trouverez ci-dessous quelques exemples courants de types d'auteurs de cybermenace et de vecteurs d'attaque courants que vous pourriez rencontrer.

| Type de menace | Niveau de sophistication | Motivation |
|---|---|---|
| **État-nation ou état parrainé** | Élevée | Intérêts géopolitiques |
| **Cybercriminels** | Modéré | Gain financier |
| **Hacktivistes, groupes terroristes et amateurs de sensations fortes** | Faible | La perturbation, causant des dommages à la réputation, pourrait être motivée par l'idéologie |
| **Menaces internes** | Faible. Les menaces internes n'utilisent généralement pas d'outils ou de techniques sophistiqués, mais sont dangereuses en raison de leur accès privilégié ou de leurs connaissances privilégiées. | Rancune contre l'organisation |

Vecteurs d'attaque courants (types d'attaques) :

- l'intrusion dans le réseau
- les vulnérabilités du jour zéro
- le logiciel malveillant
- le déni de service (DoS)
- le déni de service distribué (DDoS)
- l'ingénierie sociale
- l'hameçonnage
- l'harponnage
- les attaques par voie latérale

# Étape 3 : Créer un profil actuel

Après avoir défini le paysage cybernétique, vous devez évaluer et comprendre la position et les capacités actuelles de votre organisation.

Pour ce faire, vous utilisez un cadre ou un outil d'évaluation normalisé pour mesurer la maturité de votre organisation. L'utilisation d'un cadre de référence normalisé peut vous aider à élaborer des évaluations plus fiables et à faciliter la comparaison de vos évaluations avec les normes du secteur. De nombreux cadres d'autorités de cybersécurité réputées existent pour fournir un langage commun pour les normes et les contrôles.

**Résumé de l'étape 3 :**

- Choisissez votre cadre
- Assurez-vous d'avoir l'adhésion et personnalisez le cadre au besoin
- Mesurer l'état actuel

**L'outil d'auto-évaluation de la cybersécurité des STI de Transports Canada** est un outil que vous pouvez utiliser pour évaluer votre posture en matière de cybersécurité. Il comprend un questionnaire qui suit chacune des fonctions du NIST et établit un niveau de maturité selon l'échelle CMMI. L'outil explore plusieurs facettes de l'ingénierie de la sécurité, notamment la culture, la gestion, les processus et les contrôles.

Toutes les directions ou équipes concernées doivent s'entendre sur le cadre utilisé et participer à l'établissement du profil de l'état actuel. Pour les propriétaires et les exploitants d'infrastructures routières, les équipes de TO doivent être incluses pour s'assurer que les TO sont représentés dans l'évaluation.

Une fois votre cadre d'évaluation choisi, évitez d'en modifier fréquemment la configuration. Dans certains cas, l'adaptation d'un cadre d'évaluation existant peut permettre une mesure plus efficace ou être plus pertinent pour les principaux intervenants internes. Toutefois, évitez d'apporter des modifications majeures à un cadre standard du secteur. D'ailleurs, l'utilisation d'un cadre standard facilitera la comparaison de vos résultats avec ceux d'organisations similaires. Cependant, soyez prudent lorsque vous comparez avec des organisations utilisant des cadres d'évaluation différents ou personnalisés.

**Utilisation de l'outil d'autoévaluation de la cybersécurité des STI de Transports Canada**

L'objectif de l'outil d'auto-évaluation de la cybersécurité est de donner aux propriétaires et exploitants d'infrastructures routières et aux opérateurs des SGT un moyen d'obtenir un « instantané » de la cybermaturité de votre organisation. Cette auto-évaluation vous aidera à comprendre votre état actuel en matière de cybersécurité, conformément au cadre de cybersécurité du NIST.

Les instructions complètes d'utilisation de l'outil sont disponibles en cliquant sur le lien ci-dessus. Vous pouvez également ajuster l'outil en fonction des besoins uniques de votre organisation, au besoin.

## Comprendre l'échelle d'intégration du modèle de maturité des capacités (CMMI)

L'outil d'auto-évaluation de la cybersécurité mesure le score de maturité de votre organisation, selon l'échelle CMMI. Les niveaux de maturité sont définis ci-dessous.

1. **Initiale**

Les processus à ce niveau ne sont généralement pas documentés et changent. Ils ont tendance à être conduits au besoin, de manière incontrôlée et réactive.

Les organisations de ce niveau ont généralement une connaissance limitée des risques de sécurité et une approche de gestion des risques incohérente au niveau organisationnel.

2. **Reproductible**

Les processus (procédures permettant de réaliser des activités spécifiques de cybersécurité) sont documentés et reproductibles avec des résultats constants, mais leur application peut varier d'une équipe ou d'une unité opérationnelle à l'autre. La discipline relative aux processus est présente, mais pas encore rigoureuse ni standardisée à l'échelle de l'organisation. De plus, il manque des politiques formelles et globales ainsi qu'une approche coordonnée de la gestion de la cybersécurité.

3. **Défini**

Des processus normalisés définis et documentés sont établis et peuvent être améliorés au fil du temps.

Les organisations de ce niveau ont mis en place des politiques de sécurité à l'échelle de l'organisation, avec un cycle d'examen défini.

4. **Géré**

À l'aide de mesures de contrôle et de processus, la direction peut contrôler efficacement les processus.

Les organisations de ce niveau ont officiellement défini des paramètres pour tous les processus et contrôles de sécurité. Les paramètres sont examinés pour évaluer l'efficacité des contrôles. Les processus sont intégrés au niveau organisationnel, de telle sorte qu'un changement sur un processus déclenchera un changement sur tous les processus dépendants. À ce niveau, les processus et contrôles de cybersécurité sont mesurés et suivis activement à l'aide d'indicateurs de rendement définis. La direction utilise ces indicateurs pour évaluer l'efficacité, identifier les lacunes et orienter la prise de décision.

Les organisations de ce niveau ont formellement établi des indicateurs pour leurs processus et contrôles de sécurité clés et les examinent régulièrement afin de s'assurer de leur bon fonctionnement.

**5. Optimisé**

L'accent est mis sur l'amélioration continue de la performance des processus grâce à des changements ou des mises à niveau technologiques.

Les organisations de ce niveau effectuent des analyses régulières pour identifier les faiblesses systémiques et mettre en œuvre des améliorations avant que des incidents majeurs ne surviennent. Les indicateurs sont constamment révisés et optimisés afin de faciliter des décisions éclairées en matière de risques. L'automatisation peut être utilisée, le cas échéant, pour améliorer l'efficacité et la cohérence, mais la caractéristique déterminante de ce niveau est une culture d'apprentissage et d'adaptation continus.

# Étape 4 : Faire une évaluation des risques

Cette étape vise à dresser un portrait précis des cyberrisques de votre organisation et s'appuie sur les vulnérabilités que vous avez identifiées à l'étape 2 et sur la posture cybernétique actuelle de votre organisation telle qu'évaluée à l'étape 3.

Les évaluations des cyberrisques partagent bon nombre des concepts de base avec d'autres pratiques de gestion des risques. Le risque est une combinaison d'impact et de probabilité.

- **La probabilité** décrit la probabilité que le risque se produise
- **L'impact** est une estimation mesurable des pertes potentielles liées à un risque. Elle peut être liée à divers facteurs, notamment la taille de la population touchée, les types de circulation dans l'environnement et le débit des routes

En explorant ces dimensions du risque, votre organisation peut filtrer les scénarios d'impact improbable ou minime et prioriser les risques potentiellement imminents et susceptibles de causerdes dommages importants à votre organisation.

Pour estimer ces valeurs, vous devriez inclure des représentants de toutes les unités opérationnelles concernées et avoir accès à des sources fiables de renseignements sur les menaces. Nous fournissons quelques ressources à la fin du document, dans l'encadré « Ressources supplémentaires du CCC ».

Les évaluations des risques comprennent l'évaluation de la probabilité et de l'impact, les stratégies d'atténuation et les personnes responsables des mesures. Ceux-ci sont consignés dans un registre des risques, qui est une liste de tous les risques et vulnérabilités identifiés par votre organisation.

Les évaluations des risques sont un élément essentiel d'une stratégie de gestion des risques d'entreprise (GRE), une approche intégrée visant à gérer l'ensemble des risques auxquels votre organisation peut être confrontée. Vérifiez si votre

**Résumé de l'étape 4 :**

- Choisissez une norme d'évaluation des risques. Ensuite, mettez-le en œuvre et utilisez-la
- Créer un modèle de registre des risques pour tous les risques
- Définissez la tolérance au risque et l'appétit pour le risque de votre organisation
- Intégrez la gestion des cyberrisques à votre système de gestion des risques d'entreprise
- Les évaluations des risques sont effectuées sur une base continue et comprennent l'évaluation de l'impact et de la probabilité des risques

organisation a déjà une stratégie de GRE et, le cas échéant, comment les cyberrisques peuvent y être intégrés.

La **figure 2** illustre comment intégrer la gestion des cyberrisques à la stratégie de GRE de votre organisation. Le document NIST IR 8286, « Intégration de la cybersécurité et de la gestion des risques d'entreprise », fournit des indications supplémentaires à ce sujet.

Dans le cadre de l'élaboration de cette stratégie, votre organisation définira sa tolérance au risque, ce qui permettra ensuite d'orienter les évaluations des risques cybernétiques..

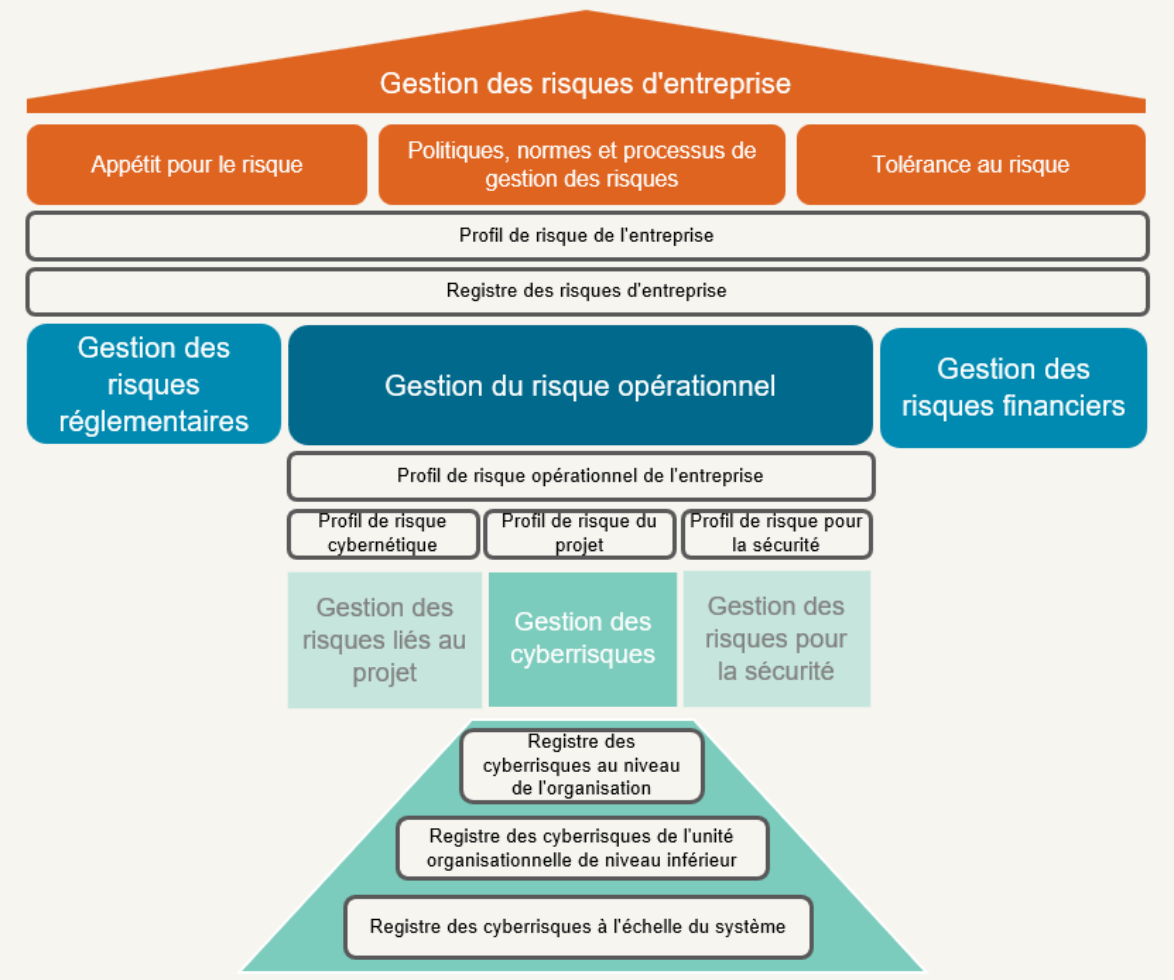
ⓘ L'outil d'autoévaluation de la cybersécurité des STI comprend un questionnaire pour vous aider à déterminer la tolérance au risque de votre organisation. Un profil cible plus bas indique une tolérance au risque plus élevée et un profil cible plus élevé indique un niveau de tolérance au risque plus faible.

Voir l'étape 5 pour plus d'information sur l'évaluation du profil cible.

Vous devez choisir une norme d'évaluation des risques établie (comme NIST SP 800-30 (en anglais) ou la méthodologie harmonisée d'évaluation des menaces et des risques) pour vous assurer que le processus d'évaluation des risques a un haut degré d'intégrité.

Enfin, des évaluations des risques devraient être intégrées à la culture de votre organisation et effectuées régulièrement, par exemple une ou deux fois par année, à mesure que les systèmes s'améliorent et que l'environnement opérationnel change. Vos premières évaluations devraient avoir une portée générale. Au fur et à mesure que vous commencez à mieux comprendre les risques, vous pouvez effectuer des évaluations plus précises grâce à des registres de risques créés à des niveaux plus granulaires.

**Figure 2 : Exemple d'intégration de la cybersécurité dans la gestion des risques organisationnels**




## Plus de conseils sur la gestion des risques liés aux TO

La gestion du réseau est un contrôle essentiel pour la sécurité des systèmes opérationnels, qui peut être entreprise par une équipe différente qui gère les actifs de TI et de TO.

S'assurer que les réseaux TI et TO sont segmentés avec des interfaces contrôlées et instrumentées est le strict niveau de protection minimum. Il est également important que le personnel qui gère le réseau soit au courant des exigences des deux interfaces.

La propagation de logiciels malveillants ou de cyberattaques entre les TO et les TI (et vice versa) est un risque sérieux que vous devez gérer. Les logiciels malveillants peuvent arriver via une interface réseau directe, des supports portables ou un accès à distance.

Lors de la gestion des interfaces entre les réseaux TO et TI, les organisations appliquent généralement l'une des deux grandes approches conceptuelles suivantes pour déterminer comment la confiance, la segmentation et les contrôles de sécurité sont mis en œuvre.

1. **Séparation stricte (approche « zéro confiance »).** Cette approche considère par défaut tous les réseaux externes ou interconnectés comme non fiables. Une segmentation forte et des interfaces étroitement contrôlées sont utilisées pour minimiser le risque de propagation de logiciels malveillants ou d'accès non autorisés entre les réseaux. Cette approche peut s'avérer efficace pour protéger les environnements TO sensibles, mais elle peut nécessiter des ressources supplémentaires et limiter la flexibilité opérationnelle si elle n'est pas soigneusement conçue.

2. **Segmentation basée sur les risques (contrôles proportionnels).** Cette approche applique des contrôles de sécurité en fonction d'une évaluation du risque relatif entre les réseaux. Les contrôles sont adaptés à des facteurs tels que la criticité du système, son exposition et les protections existantes, permettant ainsi aux organisations d'équilibrer sécurité et efficacité opérationnelle. Bien que plus flexible, cette approche repose sur une évaluation précise des risques et une surveillance continue, et peut être moins efficace si les risques sont sous-estimés.

# Étape 5 : Créer un profil cible

Si vous avez une bonne compréhension du profil de risque actuel de votre organisation, vous pouvez déterminer le profil cible de votre organisation (en d'autres termes, l'état souhaité de votre organisation pour qu'elle soit en position de force pour gérer ses risques).

Le profil cible vous aidera à identifier les écarts entre votre état actuel et votre état cible, et vous aidera à créer des plans d'action viables.

L'outil d'auto-évaluation de la cybersécurité des STI comprend une évaluation du profil cible qui vous aidera à définir l'état souhaité en fonction des besoins de sécurité de votre organisation.

**Résumé de l'étape 5 :**

- Créez un profil cible basé sur les facteurs pertinents et les informations les plus récentes

Cet outil vous donnera un point de départ, mais une personnalisation plus poussée au niveau de la catégorie ou même de la sous-catégorie peut être envisagée par des experts au sein de l'organisation.

Maximiser les scores dans tous les domaines de l'outil n'est pas réaliste pour la plupart des organisations. Dans le contexte de l'échelle CMMI utilisée dans l'outil d'auto-évaluation, une note de 5 dans n'importe quelle capacité est extrêmement difficile à atteindre, et même les organisations les plus matures auraient de la difficulté à l'atteindre et à la maintenir. Il est donc judicieux de fixer des objectifs réalistes. Par ailleurs, un score élevé dans un domaine, associé à des scores faibles dans d'autres, peut signifier que vous vous êtes trop engagé dans un domaine spécifique et que vous devez vous concentrer sur d'autres domaines.

Enfin, vous devez définir vos cibles de départ en utilisant la même échelle que le profil d'état actuel de l'étape 3, comme l'échelle CMMI utilisée dans l'outil d'autoévaluation de la cybersécurité.

ⓘ L'outil d'autoévaluation de la cybersécurité des STI vous permet de modifier manuellement votre profil cible pour chaque sous-catégorie. Vous pouvez fixer des niveaux de maturité cibles de 2 à 5.

Pour les sous-catégories dont les scores actuels sont inférieurs au niveau 3, nous recommandons de fixer le niveau 3 comme niveau cible minimal. L'étape 6 fournit plus de conseils sur le passage d'un niveau 1 à un niveau 3.

## Déterminer votre profil cible

L'outil d'autoévaluation de la cybersécurité des STI vous aidera à établir votre profil actuel et votre profil cible. Ensuite, vous comparerez ces deux situations pour identifier les lacunes potentielles les plus importantes au sein de votre organisation.

L'évaluation du profil cible comporte une série de questions qui vous aideront à établir un état cible en fonction de la taille de votre organisation, de la communauté que vous desservissez et du type de technologie que vous avez en service.

L'évaluation tient compte de facteurs tels que :

- le nombre de personnes dans votre province ou territoire
- les kilomètres de routes dans votre province ou territoire
- le débit du trafic dans votre province ou territoire
- la connaissance des exigences réglementaires
- le pourcentage du budget de TI consacré à la cybersécurité
- le nombre d'employés à temps plein dédiés à la cybersécurité dans votre organisation
- les cyberattaques récentes
- le technologies STI actuellement utilisées
- la mise en œuvre prévue des technologies STI au cours des 5 prochaines années
- la quantité d'équipement gérée par votre organisation
- l'objectif d'affaires
- les résultats de sécurité souhaités
- la tolérance au risque idéale
- la compréhension du paysage actuel des menaces
- l'existence d'une stratégie globale de cyberrisque dans votre organisation
- les politiques de gestion des fournisseurs

Une fois que vous avez défini un état cible initial, vous pouvez l'ajuster au fil du temps. Vous pouvez le faire en :

- augmenter ou diminuer le score de chaque sous-catégorie par incréments de 0,5 point
    - Si vous pensez que le profil suggère une cible plus basse ou plus élevée dans tous les domaines, vous pouvez l'utiliser pour augmenter ou diminuer rapidement les scores de l'état cible
    - Un profil cible de 3,5 ou 4,5 augmentera les scores cibles pour toutes les sous-catégories des fonctions Identité et Protection (à 4 ou 5 respectivement) et laissera les autres à 3 ou 4
- ajuster manuel de votre pointage
    - Si vous voulez un contrôle total de votre profil cible, vous pouvez définir manuellement les scores pour les sous-catégories

# Étape 6 : Déterminer, analyser et prioriser les lacunes

La différence entre le profil cible de votre organisation et le profil actuel vous aidera de cerner les lacunes dans les processus, les politiques et les contrôles.

L'échelle CMMI fournit une mesure quantitative de ces lacunes, et l'outil d'autoévaluation de la cybersécurité des STI recommande des contrôles qui peuvent aider à combler les lacunes. Assurez-vous de faire des pas lents et progressifs vers votre état cible.

Par exemple, si votre organisation est au niveau 1 pour une question et que votre état cible est le niveau 3 pour ces contrôles, n'ayez pas peur d'apporter de petites améliorations graduelles qui augmenteraient votre maturité à un niveau 2 pendant un certain temps. Tenter de faire de grands sauts de maturité peut être difficile à planifier et à exécuter et peut entraîner des retards et des augmentations de coûts.

**Résumé de l'étape 6 :**

- Analyser les lacunes selon la probabilité et l'impact estimés
- Faire une analyse coûts-avantages pour prioriser les lacunes

L'outil met en évidence l'ampleur relative des lacunes pour les différentes capacités, ce qui peut aider votre organisation à prioriser le travail. L'outil et l'annexe A du Guide de l'utilisateur de l'outil d'auto-évaluation de la cybersécurité des STI comprennent des recommandations de contrôles, mais le choix des contrôles à mettre en œuvre vous obligera à évaluer les objectifs, les risques et les ressources de votre organisation. Une analyse coûts-avantages (illustrée dans la section suivante) peut aider à déterminer les activités qui ont le plus d'impact sur le niveau d'investissement disponible.

Suite à une analyse coûts-avantages, vous devrez peut-être prendre des décisions d'optimisation. Certaines améliorations peuvent coûter plus cher que votre budget disponible, et vous devez veiller à ce que le financement de ces activités ne se fasse pas au détriment de la capacité d'une organisation à maintenir sa position de risque.

Dans ces cas, les petits projets peuvent être préférables, car ils comportent moins de risques. Le groupe de travail sur la cybersécurité devrait travailler avec les intervenants financiers et de gestion pour créer un plan qui correspond au niveau d'aisance de votre organisation à l'égard de la cybersécurité et des risques financiers.

Les projets de plus grande envergure doivent se voir attribuer une combinaison d'IRC et de jalons afin que le groupe de travail puisse surveiller la façon dont le plan est mis en œuvre à l'étape 7.

**Analyse coûts-avantages**

Il existe de nombreuses façons de faire une analyse coûts-avantages. Deux sont soulignées ci-dessous : une méthode simple fondée sur la finance et une méthode plus complexe fondée sur le risque.

Dans les deux cas, vous devrez calculer le coût de mise en œuvre de votre plan, qui peut inclure :

- le coût initial de la mise en œuvre
- les coûts d'entretien sur une période déterminée;
- le coût de la perte de productivité ou de ressources;
- le coût de la détermination de la faisabilité

Lors du calcul des coûts d'entretien, la période pertinente doit être cohérente avec la façon dont la probabilité est calculée. Ainsi, si un risque est susceptible de se produire au cours des 6 prochaines années, l'étendue des coûts d'entretien serait de 6 ans.

Lorsque vous déterminez le coût de la perte de productivité ou de ressources, assurez-vous que tous les intervenants sont consultés pour s'assurer que les impacts imprévus ne sont pas négligés.

**Méthode fondée sur le financement**

Une analyse financière évalue les risques en fonction de l'incidence financière estimée avant et après la mise en œuvre. Chaque processus, politique ou contrôle correspond généralement à l'une des sous-catégories de l'annexe A du Guide de l'utilisateur de l'outil d'autoévaluation de la cybersécurité des STI.

Un faible rapport coûts-avantages indique un impact relatif plus élevé, ce qui signifie que vous devez prioriser l'élément, tandis qu'un rapport coûts-avantages élevé indique que les coûts de mise en œuvre sont élevés par rapport à la valeur possible.

**Tableau 2 : Exemple d'analyse coûts-avantages à l'aide d'une méthode financière**

| Processus, politique ou contrôle | Incidence financière du risque actuel | Incidence financière estimée après la mise en œuvre | Delta du risque [1] | Coût de mise en œuvre | Rapport coûts/avantages [2] |
|---|---|---|---|---|---|
| Contrôle A | 100 000 $ | 20 000 $ | 80 000 $ | 200 000 $ | 2.5 |

**[1] Delta du risque** = Incidence financière du risque actuel - Incidence financière estimée après la mise en œuvre

**[2] Rapport coûts/avantages** = Coût de mise en œuvre / Delta du risque

**Méthode fondée sur le risque**

Cette méthode tient compte de divers facteurs fondés sur le risque, y compris la probabilité et l'impact. Vous devrez utiliser une matrice ou un cadre pour vous assurer que votre analyse est cohérente, comme l'échelle d'évaluation du NIST SP 800-30 (en anglais) (résumée dans le tableau 4.7.2).

**Tableau 3 : Exemple d'échelle d'évaluation**

| Niveau de risque | Score | Descriptif |
|---|---|---|
| Très élevé | 10 | **Un risque très élevé** signifie qu'un événement de menace pourrait avoir **de multiples effets négatifs graves ou catastrophiques** sur les activités de l'organisation, les actifs organisationnels, les personnes, d'autres organisations ou le pays |
| Élevée | 8 | **Risque élevé** signifie qu'un événement de menace pourrait avoir un effet **négatif grave ou catastrophique** sur les activités organisationnelles, les actifs organisationnels, les personnes, d'autres organisations ou le pays |
| Modéré | 5 | **Un risque modéré** signifie qu'un événement de menace pourrait avoir un effet **négatif grave** sur les activités organisationnelles, les biens organisationnels, les personnes, d'autres organisations ou le pays |
| Faible | 2 | **Un risque faible** signifie qu'un événement de menace pourrait avoir un effet **négatif limité** sur les opérations organisationnelles, les actifs organisationnels, les personnes, les autres organisations ou le pays |
| Très faible | 0 | **Un risque très faible** signifie qu'un événement de menace pourrait avoir un effet **négatif négligeable** sur les opérations organisationnelles, les actifs organisationnels, les personnes, d'autres organisations ou le pays |

Votre organisation peut également créer sa propre matrice. Le tableau 4 illustre comment une analyse coûts-avantages peut être effectuée à l'aide de l'échelle d'évaluation du tableau 3.

**Tableau 4 : Exemple d'analyse coûts-avantages à l'aide d'une méthode fondée sur les risques**

| Processus, politique ou contrôle | Risque actuel | Risque estimé après la mise en œuvre | Delta du risque [1] | Coût de mise en œuvre | Rapport coûts/avantages [2] |
|---|---|---|---|---|---|
| Contrôle A | Élevée (8) | Faible (2) | 6 | 200 000 $ | 33,333.33 |

**[1] Delta du risque** = Risque actuel - Risque estimé après la mise en œuvre

**[2] Rapport coûts/avantages** = Coût de mise en œuvre / Delta du risque

La mise en œuvre d'un contrôle serait fondée sur l'ampleur relative du rapport coûts-avantages de tous les contrôles. Dans certains cas, la gestion d'un risque peut être trop coûteuse. Dans cette situation, votre organisation devrait réduire le risque aussi bas que possible, ce qui signifie que les dommages d'un risque potentiel devraient être réduits autant que possible, compte tenu des contraintes organisationnelles.

# Étape 7 : Mettez en œuvre votre plan d'action

La mise en œuvre de votre plan d'action peut impliquer des investissements, des projets et des engagements en matière de ressources, petits et importants.

Pour commencer à mettre en œuvre votre plan d'action, il est essentiel d'obtenir le soutien de la direction et établissez un budget avant d'effectuer l'action, le contrôle ou le traitement des risques identifiés. Ce processus peut être complexe. Voici quelques méthodes pour vous aider à obtenir ce soutien :

- **Élaborer une analyse de rentabilisation :** résumez les risques et les avantages, en vous basant sur les résultats de l'étape 6, et insistez sur le retour sur investissement. Ce résumé peut être intégré dans un document d'analyse de rentabilité.
- **Intégrer la cybersécurité aux objectifs de l'organisation :** présentez-la comme un levier de croissance, et non comme un simple enjeu technique, en démontrant comment elle contribue à la sécurité, à la fiabilité, à la conformité et à la réputation de l'entreprise.
- **S'appuyer sur des normes externes :** référez-vous aux référentiels CCC et NIST pour renforcer votre crédibilité.
- **Échelonner les demandes de financement :** commencez par des projets de plus petite envergure, assortis d'étapes réalisables, afin de créer une dynamique positive et d'instaurer un climat de confiance.

**Résumé de l'étape 7 :**

- Déterminer, approuver et mettre en œuvre des plans d'action
- Surveiller les plans d'action et les risques associés au fil du temps à l'aide d'IRC et de jalons
- Attribuer le plan d'action de mise en œuvre au secteur avec les experts appropriés

Pour tous les plans d'action, vous devez continuer à surveiller le travail pour vous assurer que la mise en œuvre est soutenue et que les résultats sont atteints de façon continue.

Le groupe de travail sur la cybersécurité devrait collaborer avec la direction de votre organisation pour superviser la mise en œuvre du plan d'action, mais devrait également déléguer des activités particulières à des experts du secteur, le cas échéant.

Par exemple, le travail d'exécution d'un programme de TO peut être surveillé par le groupe de travail sur la cybersécurité au moyen d'IRC et de suivi des jalons, mais des ingénieurs spécialisés en TO peuvent être nécessaires pour effectuer le travail réel.

Les travaux doivent tenir compte des exigences en matière de confidentialité, d'intégrité et de disponibilité des systèmes et des données à toutes les étapes. Par exemple, tout « temps d'arrêt » nécessaire pour apporter des changements doit être mis en balance avec l'impact sur la disponibilité de la cyberattaque contre laquelle il se défend.

Lors de la mise en œuvre des plans d'action, les progrès vers la maturation de la posture de cybersécurité de l'organisation peuvent être surveillés en mettant à jour régulièrement le profil actuel et en le comparant par la suite au profil cible. Vous pouvez réutiliser l'outil d'autoévaluation de la cybersécurité des STI pour cet exercice.

# Amélioration continue après avoir atteint l'état cible

La cybersécurité est une cible mouvante. Les menaces et les vulnérabilités évoluent constamment et exigent que les organisations s'adaptent et réagissent de manière tout aussi dynamique. Atteindre votre objectif ne doit pas être une fin en soi, mais le point de départ d'une amélioration continue. Pérenniser ces progrès nécessitera des investissements constants, un engagement fort de la direction et une culture d'entreprise qui intègre la cybersécurité au cœur des priorités stratégiques.

Des revues et des mises à jour régulières sont essentielles, mais la fréquence doit correspondre aux ressources et au profil de risque de votre organisation. L'amélioration n'a pas besoin d'être linéaire ; l'important est de maintenir l'élan et d'intégrer la cybersécurité dans les processus décisionnels quotidiens. Célébrer les étapes importantes et communiquer régulièrement sur les progrès réalisés aide à maintenir l'engagement et la motivation des parties prenantes.

En suivant les étapes décrites dans ce guide, vous garderez à jour votre compréhension des menaces, des risques et des vulnérabilités, ce qui éclairera vos plans et actions futurs. La réussite repose sur des données précises et à jour, ainsi que sur la collaboration, en tirant parti des bases de données sur les vulnérabilités, des renseignements sur les menaces et du partage d'informations avec des organisations homologues.

Pour obtenir des conseils et des alertes fiables, le Centre canadien pour la cybersécurité (CCC) est une ressource essentielle. Le CCC offre des conseils, des services et des notifications de menaces pour aider les organisations à renforcer leur résilience. Consultez le tableau des ressources à la fin de ce document pour des exemples d'outils et de publications du CCC.

# Ressources supplémentaires du CCC

**Alertes et avis**

Le CCC émet des alertes et des avis sur les cybermenaces, les vulnérabilités ou les incidents potentiels, imminents ou réels touchant les infrastructures essentielles du Canada.

https://www.cyber.gc.ca/fr/alertes-avis

**Signaler un cyberincident**

Le signalement d'un cyberincident aide le CCC à assurer la sécurité du Canada et des Canadiens en ligne. Vos renseignements permettront au CCC de fournir des conseils, des directives et des services en matière de cybersécurité. Le signalement au CCC ne déclenchera pas une intervention immédiate des organismes d'application de la loi, comme des enquêtes sur la cybercriminalité ou d'autres infractions criminelles.

https://www.cyber.gc.ca/fr/cyberincidents

**Publications**

Ces documents d'orientation comprennent des recommandations et des mesures que votre organisation peut mettre en œuvre pour protéger vos réseaux, vos systèmes et vos informations.

https://www.cyber.gc.ca/fr/orientation

**Assemblyline – Analyse et de détection de maliciels**

Ce service permet aux partenaires de divulguer et d'échanger des échantillons de logiciels malveillants avec le CCC. Le service permet d'obtenir des résultats rapides et automatisés qu'une organisation peut intégrer à ses processus internes de cybertriage.

https://www.cyber.gc.ca/fr/outils-services/chaine-montage-assemblyline

**Système national de notification des cybermenaces**

Ce système avise les organisations canadiennes des services mal configurés, des vulnérabilités et de l'infrastructure compromise sur leur espace IP. Les avis sont fondés sur les données reçues des sources ouvertes et des flux de menaces commerciaux et fiables et du CCC.

https://www.cyber.gc.ca/fr/orientation/evaluation-cybermenaces-nationales-2025-2026

**Équipe des partenariats avec le secteur des transports**

Pour vous inscrire à la liste de distribution de l'équipe des partenariats du secteur des transports du CCC, veuillez envoyer un courriel à : transport-par@cyber.gc.ca.

Si vous souhaitez en savoir plus sur les services avancés du CCC, contactez-nous en envoyant un courriel à contact@cyber.gc.ca.