Secrétariat du Conseil du Trésor du Canada
Treasury Board of Canada Secretariat
Canada

Lignes directrices sur la gestion des vulnérabilités du gouvernement du Canada

Publié : le 2025-11-17

Publié par le Secrétariat du Conseil du Trésor du Canada
90 rue Elgin, Ottawa, Ontario, K1A 0R5, Canada

No de catalogue BT22-293/2025F-PDF
ISBN: 978-0-660-97558-0

Ce document est disponible sur Canada.ca, le site Web du gouvernement du Canada.

Ce document est disponible en médias substituts sur demande.

Nota : Pour ne pas alourdir le texte français, le masculin est utilisé
pour désigner tant les hommes que les femmes.

Also available in English under the title: Government of Canada Guideline on Vulnerability Management

Lignes directrices sur la gestion des vulnérabilités du gouvernement du Canada

Sur cette page

1. Introduction

▼ Dans cette section

1.1 Contexte

La Politique sur la sécurité du gouvernement et l'Annexe B : Procédures obligatoires relatives aux mesures de sécurité de la technologie de l'information de la Directive sur la gestion de la sécurité exigent que les ministères mettent « en œuvre des mesures pour protéger les systèmes d'information, leurs composants et l'information qu'ils traitent et transmettent contre les attaques qui exploitent les vulnérabilités dans les systèmes d'information pour toucher leur intégrité et qui pourraient avoir une incidence sur leur disponibilité ou leur confidentialité (par exemple un code malveillant) [1] ». Cette exigence comprend la mise en œuvre de mesures correctives, comme l'application de correctifs, pour remédier aux vulnérabilités. De plus, le Centre canadien pour la cybersécurité classe l'application de correctifs aux applications et aux systèmes d'exploitation en deuxième place dans sa liste des plus importantes mesures de sécurité des technologies de l'information (TI) que les organisations peuvent prendre pour réduire au minimum les intrusions et les répercussions connexes [2].

Ce document présente les éléments fondamentaux du modèle de maturé de la gestion des vulnérabilités (en anglais) du SANS Institute ainsi que du guide de planification de la gestion des correctifs d'entreprise : maintenance préventive des technologies (NIST SP 800-40 Rev. 4) (en anglais) pour les technologies de gestion des correctifs d'entreprise. Il fournit des conseils précis sur la mise en place, la tenue à jour et la gestion d'un programme de gestion des correctifs et des vulnérabilités.

La gestion des vulnérabilités (GV) est à la base une fonction de gestion des risques conçue pour cerner, évaluer et atténuer les risques liés à la sécurité de l'information découlant des faiblesses des TI. En mettant l'accent sur la correction ou la réduction des risques à des niveaux acceptables, la GV permet à une organisation d'assurer la continuité de sa mission de façon efficace et sécuritaire. La GV sert à réduire le risque d'exploitation d'une manière exigeant beaucoup moins de temps et de ressources financières que le fait de réagir à un incident après l'exploitation. Ainsi, un programme de GV bien mis en œuvre vise à optimiser la gestion des risques et l'affectation des ressources.

1.2 Objectif et portée

Le présent document vise à fournir des conseils sur la mise en place, la tenue à jour et la gestion d'un programme de GV au sein d'un ministère ou d'un organisme du gouvernement du Canada (GC).

Les présentes lignes directrices cadrent avec les documents et instruments du GC suivants :

- Politique sur la sécurité du gouvernement;
- Politique sur les services et le numérique;
- Directive sur la gestion de la sécurité;
- Stratégie intégrée de cybersécurité du gouvernement du Canada;
- Plan de gestion des événements de cybersécurité du gouvernement du Canada (PGEC GC);
- Orientation sur la gestion des rustines;
- Correction des systèmes d'exploitation et des applications – Bulletin de sécurité des TI à l'intention du gouvernement du Canada (ITSM-96)

1.3 Public cible

Les présentes lignes directrices s’adressent aux personnes responsables de la gestion, de l’analyse et de la correction des vulnérabilités qui touchent les systèmes de TI du GC. Ces responsables comprennent les gestionnaires des risques liés à la cybersécurité, les équipes de GV, les responsables des services de TI, les administrateurs des services de TI et les agents de sécurité des TI.

2. Survol de la gestion des vulnérabilités

▼ Dans cette section

Figure 2.1 – Éléments d’un programme de gestion des vulnérabilités

Les éléments essentiels d'un programme efficace de GV comprennent ce qui suit.

- **Gouvernance :** des processus de gouvernance et des instruments de politique bien définis servent de fondement à toutes les activités de GV. Une communication et une coordination efficaces entre les diverses équipes, y compris celles des TI, de la sécurité et du développement, sont essentielles. La tenue de réunions régulières et la mise en place de cadres de collaboration aident à combler les écarts entre les équipes afin de favoriser une approche unifiée des questions de sécurité.

- **Compréhension des dépendances opérationnelles des actifs de TI :** une GV efficace exige une connaissance exhaustive et à jour de l'état des actifs de TI (c'est-à-dire les stocks et les configurations) et de la façon précise dont ils assurent la tenue d'activités opérationnelles et peuvent donc mettre celles-ci en péril.
- **Détection des vulnérabilités :** diverses méthodes comme les analyses de réseau, les agents, les essais de pénétration, la gestion de la surface d'attaque, l'analyse des composants logiciels ainsi que l'information fondée sur les fournisseurs et le renseignement sont essentielles pour cerner les vulnérabilités dans les systèmes d'une organisation. Un mécanisme officiel et coordonné de divulgation des vulnérabilités permet une meilleure compréhension.
- **Évaluation des risques liés aux vulnérabilités :** les vulnérabilités doivent être classées par ordre de priorité en fonction du niveau de risque qu'elles présentent pour les activités opérationnelles. Une approche fondée sur le risque devrait être utilisée pour évaluer la gravité et l'incidence possible des vulnérabilités, pour que la priorité soit ainsi accordée aux menaces les plus graves. Un cadre de gestion des risques doit fournir une méthode transparente, raisonnable et reproductible pour établir la priorité des vulnérabilités et présenter les délais d'atténuation connexes.
- **Activités d'atténuation :** le processus d'évaluation des risques devrait présenter les exigences de travail sous forme de correctifs et d'autres mesures d'atténuation. Des échéanciers clairs pour la correction des vulnérabilités devraient être définis en fonction des niveaux de risque afin d'assurer une atténuation rapide des vulnérabilités à risque élevé et le respect continu des exigences réglementaires. Ce travail devrait s'accomplir par l'intermédiaire de la création de billets, de la gestion du changement, de la gestion de la configuration et des outils de gestion des correctifs.

- **Mesures, rapports et conformité :** des mesures et une production de rapports solides sur les activités de GV sont essentielles à l'amélioration continue et à la responsabilisation.

2.1 Gouvernance

Une GV efficace repose sur des instruments de politique et des processus de gouvernance bien définis. Ils établissent les exigences, les attentes, les responsabilités, les cadres et les processus de travail, tous approuvés par la haute direction pour assurer les ressources et le soutien institutionnels. Les documents sur la gouvernance doivent comprendre des politiques générales et des procédures tactiques intégrant les pratiques exemplaires de l'industrie. En cas de différend ou d'audit, ces documents fournissent un registre de l'engagement de l'organisation à l'égard d'une gouvernance structurée et transparente.

Voici les principaux éléments de la gouvernance en matière de GV.

- **Engagement de la direction :** un solide leadership par les cadres supérieurs (par exemple, dirigeant principal des données du ministère, dirigeant principal de la sécurité de l'information) est essentiel au succès d'un programme de GV. Les dirigeants doivent faire la promotion du programme, affecter des ressources et veiller à ce que la sécurité soit une priorité dans l'ensemble de l'organisation. L'engagement des dirigeants envoie un message clair aux employés, comme quoi la sécurité est importante, et les encourage à s'approprier le programme et à y participer.
- **Organes décisionnels et protocoles de prise de décisions :** préciser qui a le pouvoir et la responsabilité de prendre des décisions, en veillant au respect des objectifs de gestion du risque de l'organisation.
- **Évaluation des risques et atténuation :** définir des processus et des cadres pour évaluer les vulnérabilités et établir des activités

d’atténuation et des échéanciers en fonction des niveaux de risque.

- **Mesures du rendement :** utiliser des mesures pour mesurer divers aspects du programme de GV qui serviront d’indicateurs de rendement clés en matière d’amélioration continue.
- **Conformité et documents :** veiller au respect des règlements externes et des politiques internes en limitant au minimum les risques juridiques et opérationnels. Les documents aident à communiquer les processus nécessaires et à veiller à ce que tous les intervenants comprennent leurs rôles et responsabilités.
- **Éléments obligatoires et éléments recommandés :** faire une distinction claire entre les éléments obligatoires et les éléments recommandés dans les documents sur la gouvernance.
- **Ententes de niveau de service :** préciser les attentes et les ententes de niveau de service pour les services de GV, en particulier lorsqu’on fait appel à des tiers.

2.2 Compréhension des dépendances opérationnelles des actifs de TI

Il est essentiel pour la GV de comprendre les dépendances des activités opérationnelles essentielles à certains actifs de TI. Les organisations doivent avoir une connaissance approfondie des activités opérationnelles qui génèrent de la valeur et orientent leur mission. Il s’agit notamment de relever les défis uniques liés à la gestion des vulnérabilités dans les environnements infonuagiques. Des techniques d’analyse spécialisées et des contrôles de sécurité adaptés aux ressources en nuage dynamiques et partagées devraient être mis en œuvre. Pour gérer efficacement les vulnérabilités, les organisations devraient procéder au mappage entre leurs actifs de TI et leurs activités opérationnelles, et déterminer le risque opérationnel associé à chaque actif de TI. Les contrôles CM-8 et PM-5 des

Contrôles de sécurité et améliorations de contrôle suggérés (ITSG-33) du Centre canadien pour la cybersécurité mettent l'accent sur la nécessité de procéder à un mappage méthodique des activités opérationnelles par rapport aux actifs de TI sous-jacents, afin qu'ainsi l'ordre de priorité des vulnérabilités tienne compte de l'urgence technique et du risque pour les activités opérationnelles essentielles.

Le mappage des actifs de TI avec les activités opérationnelles nécessite une visibilité à jour et précise de l'écosystème technologique grâce à la découverte complète des actifs, au mappage des dépendances, au suivi des stocks en temps réel et à l'intégration aux processus et outils de gestion du changement et de la configuration de l'organisation. Les organisations doivent tenir à jour leur répertoire et les bases de données de gestion des configurations de leurs biens informatiques physiques et virtuels, y compris les actifs liés à la technologie opérationnelle et à l'Internet des objets.

La gestion des actifs de TI et la gestion des configurations permettent aux organisations de faire le suivi des logiciels non conformes déployés dans les environnements de TI. Étant donné la complexité et les multiples facettes des systèmes de TI, il est essentiel d'inclure tous les environnements informatiques dans un programme de GV, qu'il s'agisse de technologies mobiles, sur place, infonuagiques ou opérationnelles. Ces technologies comprennent notamment les points terminaux, les applications, les intergiciels, les bibliothèques, les systèmes d'exploitation, les hyperviseurs, les machines virtuelles, les moteurs de conteneurs, les conteneurs, les micrologiciels, le matériel, les systèmes de contrôle industriel, les systèmes d'acquisition et de contrôle de données, les systèmes de commande répartis, les automates programmables, les terminaux à distance, les interfaces personne-machine, les capteurs et les actionneurs.

La Politique sur les services et le numérique rend la gestion des actifs obligatoire. Pour obtenir de plus amples renseignements sur la gestion des actifs de TI, consultez la publication Utilisation de la gestion des biens de technologies de l'information (GBTI) pour renforcer la cybersécurité (ITSM.10.004) (2023) du Centre canadien pour la cybersécurité.

2.3 Détection des vulnérabilités

La détection des vulnérabilités est un élément crucial de la GV et comprend la recherche de vulnérabilités au sein des réseaux sous la responsabilité du ministère. Les organisations acquièrent des connaissances sur les vulnérabilités en synthétisant des données provenant de multiples sources, comme l'analyse des vulnérabilités, les renseignements sur les menaces, les avis des fournisseurs, les essais de pénétration et le mécanisme coordonné de divulgation des vulnérabilités. L'intégration des flux de renseignements sur les menaces aide à demeurer au fait des nouvelles vulnérabilités et menaces, ce qui permet d'établir les priorités et de corriger les vulnérabilités de manière plus pratique. Les sources offrent des renseignements uniques qui fournissent collectivement une vue d'ensemble pour cerner les vulnérabilités.

Les organisations doivent effectuer des analyses des vulnérabilités régulières et automatisées afin de toujours cerner les vulnérabilités potentielles et les autres risques de sécurité dans leurs réseaux, conformément à la Directive sur la gestion de la sécurité. Les outils automatisés doivent être configurés pour exécuter des analyses à intervalles réguliers et lorsque d'importants changements sont apportés à l'infrastructure du réseau. Des données à jour sur la GV sont essentielles pour appuyer la gestion des cyberincidents, car elles permettent une évaluation précise des répercussions potentielles ou réelles d'un incident.

Réduction des vulnérabilités au moyen d'un cycle de vie du développement logiciel

« Un **cycle de vie du développement logiciel** est une méthodologie officielle ou officieuse pour la conception, la création et la tenue à jour des logiciels (y compris le code intégré au matériel). Il existe de nombreux modèles de cycles de vie du développement logiciel, y compris les modèles en cascade, en spirale, agiles et (plus particulièrement) agiles combinés aux pratiques de développement de logiciels et d'opérations de TI (DevOps)… Quel que soit le modèle de cycle de vie du développement logiciel utilisé, des pratiques sûres de développement logiciel devraient y être intégrées pour trois raisons : réduire le nombre de vulnérabilités dans les logiciels publiés, réduire l'incidence potentielle de l'exploitation de vulnérabilités non détectées ou non corrigées, et s'attaquer aux causes profondes des vulnérabilités afin d'éviter qu'elles ne se reproduisent. Les vulnérabilités comprennent non seulement des bogues causés par des défauts de codage, mais aussi des faiblesses causées par des paramètres de configuration de sécurité, des hypothèses de confiance erronées et une analyse des risques désuète. »
(Source [traduction libre] : cadre de développement de logiciels sécurisés V1.1 : recommandations pour atténuer le risque de vulnérabilités logicielles (NIST SP 800-218) (en anglais).

Les plateformes de GV commerciales ne peuvent généralement pas détecter les défauts des applications opérationnelles personnalisées ou des applications gouvernementales standard. Le cycle de vie de la gestion des risques pour ces applications devrait comprendre des évaluations

régulières ciblées des vulnérabilités, des essais de pénétration et un processus coordonné de divulgation des vulnérabilités pour relever les lacunes logicielles et de configuration.

Les applications personnalisées reposent souvent sur des composants commerciaux standard ou de code source libre, des interfaces de programmation d'application, des progiciels ou des cadres. Les responsables d'applications doivent être au courant de ces dépendances, y compris l'utilisation d'une nomenclature logicielle et de documents sur l'architecture de la solution. Une nomenclature logicielle est un répertoire complet de tous les composants logiciels, y compris les bibliothèques, les outils et les processus utilisés dans le développement d'un produit logiciel. La nomenclature logicielle joue un rôle essentiel dans la GV en assurant la transparence de la chaîne d'approvisionnement des logiciels. Ainsi, les organisations peuvent repérer et évaluer rapidement les vulnérabilités potentielles. Lorsqu'elles sont jumelées à des outils d'analyse de la composition logicielle, les nomenclatures logicielles peuvent améliorer considérablement la sécurité en analysant les dépendances de code source libre pour repérer les vulnérabilités connues, les licences risquées et les logiciels malveillants.

2.3.1 Méthodes pour cerner les vulnérabilités

Il existe de multiples méthodes pour cerner les vulnérabilités au sein des systèmes, y compris des méthodes d'évaluation automatisées et manuelles. Voici quelques-unes des approches les plus couramment utilisées en GV.

2.3.1.1 Évaluations internes

Les organisations évaluent régulièrement les vulnérabilités au moyen d'outils ou de processus spécialisés. Les outils d'analyse automatisés analysent les plages Internet Protocol (IP) prédéfinies ou utilisent des agents installés dans les systèmes pour cerner les vulnérabilités connues. Bien que les agents permettent une analyse continue, ce ne sont pas tous les actifs (par exemple, routeurs, informatique sans serveur, appareils multifonction) qui prennent en charge l'installation d'agents. De plus, dans certains environnements, l'installation d'agents peut ne pas être possible ou permise. Les analyses peuvent être effectuées sur des actifs de production ou dans un laboratoire, et les résultats peuvent être extrapolés à l'environnement de production. Il importe de veiller à ce que les fichiers de signature des vulnérabilités soient automatiquement et régulièrement mis à jour.

Les méthodes d'évaluation internes comprennent ce qui suit.

- **Analyse des vulnérabilités :** outils automatisés qui analysent les systèmes pour détecter les vulnérabilités connues en fonction de plages IP prédéfinies ou d'agents installés.
- **Vérification de la configuration :** outils qui évaluent les configurations des systèmes et des réseaux pour assurer la conformité aux pratiques exemplaires en matière de sécurité et aux politiques organisationnelles.
- **Analyse de l'infrastructure en tant que code :** analyse du code définissant l'infrastructure (par exemple, Terraform, CloudFormation) afin de cerner les problèmes de sécurité avant le déploiement.
- **Outils de gestion des correctifs :** systèmes permettant de faire le suivi et de gérer l'application de correctifs aux logiciels et au matériel pour corriger les vulnérabilités.
- **Détection et intervention aux points terminaux :** solutions qui permettent de surveiller les menaces aux points terminaux et d'y

réagir en assurant de manière continue l'évaluation et la mise en œuvre de mesures correctives.

- **Audits de conformité :** vérifications régulières pour veiller à ce que les systèmes et les processus soient conformes aux politiques internes et aux règlements externes.
- **Analyse des journaux :** examiner les journaux des systèmes et des applications pour repérer les activités inhabituelles pouvant indiquer des vulnérabilités ou des atteintes à la sécurité.
- **Analyse du trafic réseau :** surveillance du trafic réseau pour détecter les anomalies pouvant indiquer des vulnérabilités ou des activités malveillantes.
- **Essais de pénétration :** simulation d'attaques réelles pour découvrir des vulnérabilités que les outils automatisés pourraient manquer.

2.3.1.2 Évaluations externes

Les évaluations externes comprennent la détection des vulnérabilités provenant de l'extérieur du périmètre de réseau de l'organisation. Cette approche aide à comprendre la façon dont les attaquants peuvent exploiter les faiblesses d'un point de vue externe. Les outils et services de gestion de la surface d'attaque entrent dans cette catégorie puisqu'ils aident les organisations à effectuer le mappage des actifs externes et à les surveiller. Les outils d'évaluation externes simulent le point de vue d'un attaquant en évaluant les vulnérabilités des adresses IP et des domaines externes de l'organisation. Des évaluations externes devraient être effectuées régulièrement, surtout après des changements importants à l'infrastructure du réseau.

Les méthodes d'évaluation externe comprennent ce qui suit.

- **Gestion de la surface d'attaque :** outils et services qui aident les organisations à effectuer le mappage de leurs actifs externes et à les

surveiller afin de cerner les vulnérabilités.

- **Analyse des vulnérabilités externes :** outils qui simulent le point de vue d'un attaquant en analysant les vulnérabilités des adresses IP et des domaines externes de l'organisation.
- **Évaluations par des tiers :** emploi d'entreprises de sécurité externes pour effectuer des évaluations indépendantes de la situation de sécurité externe de l'organisation.
- **Processus coordonné de divulgation des vulnérabilités :** mettre en œuvre un processus coordonné de divulgation des vulnérabilités afin de veiller à ce que les intervenants et les partenaires connaissent les vulnérabilités qui pourraient les toucher. Cette approche tire parti de l'expertise de la collectivité pour relever et gérer les enjeux de sécurité. Les programmes coordonnés de divulgation des vulnérabilités exigent des lignes directrices et des processus clairs quant à la production de rapports externes et à la communication en temps opportun avec les chercheurs.

2.3.1.3 Intervention en cas d'incident

L'intervention en cas d'incident joue un rôle dans l'amélioration des programmes de GV. Les renseignements recueillis après l'incident dans le cadre de l'examen et de l'analyse aident à comprendre comment une atteinte à la sécurité s'est produite et quelles vulnérabilités ont été exploitées. Cette analyse fournit des renseignements précieux sur les faiblesses du système, ce qui aide à établir l'ordre de priorité pour la correction des vulnérabilités qui ont été activement exploitées. Des procédures définies de divulgation des vulnérabilités améliorent la capacité à réagir aux vulnérabilités et à les corriger. Le PGEC GC inclut les vulnérabilités dans la définition d'un événement de cybersécurité, c'est-à-dire un événement, un acte, une omission ou une situation pouvant nuire à

la sécurité du gouvernement. On s’attend à ce que les ministères établissent un plan ministériel de gestion des événements de cybersécurité qui cadre avec le PGEC GC.

2.3.2 Délais d’évaluation suggérés

Pour assurer la détection rapide et efficace des vulnérabilités, les organisations devraient adopter un calendrier structuré pour chaque méthode d’évaluation. Le tableau 2.1 présente les fréquences recommandées de diverses techniques de détection des vulnérabilités, selon les directives du GC et les pratiques exemplaires de l’industrie. Ces échéanciers appuient la gestion proactive des risques et l’harmonisation avec l’évolution des menaces et des besoins opérationnels.

Tableau 2.1 : Délais d’évaluation suggérés

Méthode de détection	Fréquence recommandée	Justification ou source
Analyse des vulnérabilités (interne)	Au moins une fois par semaine ou après des changements importants; agents pour l’évaluation continue	Centre canadien pour la cybersécurité – Contrôle RA-5 de La gestion des risques liés à la sécurité des TI : Une méthode axée sur le cycle de vie (ITSG-33); cadre avec la détection proactive et les cycles de correctifs

Méthode de détection	Fréquence recommandée	Justification ou source
Analyse des vulnérabilités (externe)	Une fois par mois et après des changements importants à l'infrastructure	Appuyé par la page Facteurs relatifs à la sécurité à considérer pour les dispositifs d'accès (ITSM.80.101) du Centre canadien pour la cybersécurité et les pratiques exemplaires de l'industrie
Vérification de la configuration	Une fois par mois et après des changements de configuration	Concorde avec les contrôles CM-6 et CM-8 de La gestion des risques liés à la sécurité des TI : Une méthode axée sur le cycle de vie (ITSG-33)
Analyse de l'infrastructure en tant que code	À chaque engagement de code ou demande de retrait	Pratiques exemplaires de développement, de sécurité et d'exploitation; garantit que des vulnérabilités ne sont pas introduites avant le déploiement
Outils de gestion des correctifs	Surveillance continue; examen hebdomadaire	Garantit la mise en œuvre de correctifs en temps opportun et le respect de l'orientation du GC concernant les correctifs

Méthode de détection	Fréquence recommandée	Justification ou source
Suivi de la détection et de l'intervention aux points terminaux	En continu	Détection et intervention en temps réel; Les 10 mesures de sécurité des TI du Centre canadien pour la cybersécurité
Audits de conformité	Deux fois par année	Selon les cycles d'audit du GC et le contrôle PM-5 de La gestion des risques liés à la sécurité des TI : Une méthode axée sur le cycle de vie (ITSG-33)
Analyse des journaux	Une fois par jour ou en temps quasi réel	Selon le contrôle AU-6 de La gestion des risques liés à la sécurité des TI : Une méthode axée sur le cycle de vie (ITSG-33)
Analyse du trafic réseau	En continu	Détection des anomalies et des vulnérabilités potentielles en temps réel
Essais de pénétration	Une fois par année ou après des changements importants au système; plus fréquemment pour les systèmes à risque élevé	Selon le contrôle CA-8 de La gestion des risques liés à la sécurité des TI : Une méthode axée sur le cycle de vie (ITSG-33)

Méthode de détection	Fréquence recommandée	Justification ou source
Gestion de la surface d'attaque	En continu au moyen d'examens mensuels	Surveillance continue de l'exposition externe assurant une visibilité à jour des expositions et des actifs accessibles par Internet
Évaluations par des tiers	Une fois par année ou au besoin en fonction du risque	Garantit une validation indépendante de la situation de sécurité
Processus coordonné de divulgation des vulnérabilités	En continu; examen des rapports dans les cinq jours ouvrables suivant leur réception	PGEC GC et pratiques exemplaires de l'industrie pour une réponse rapide aux rapports externes

2.4 Évaluation des risques liés aux vulnérabilités

Les organisations du GC **doivent** « analyser les incidences des vulnérabilités cernées, et mettre en œuvre des mesures correctives (par exemple appliquer des correctifs et des mises à jour, conformément aux échéances définies et, au besoin, en cas d'urgence). » (Source : Directive sur la gestion de la sécurité, annexe B, sous-section B.2.3.7.3.)

L'évaluation efficace des risques est la pierre angulaire de tout programme de GV puisqu'elle permet aux organisations d'établir l'ordre de priorité des activités d'atténuation visant à protéger la prestation continue des activités

opérationnelles. Pour ce faire, la méthode clé à cet effet est un outil de calcul de l'évaluation des risques liés aux vulnérabilités qui devrait être conçu en fonction des principes qui suivent.

- **Facteurs de risque clairement définis :** les facteurs de risque doivent être clairement définis et être distincts les uns des autres. Parmi les exemples, on compte la facilité d'exploitation, l'exploitation active sur des réseaux, la présence sur les systèmes de TI appuyant les activités opérationnelles essentielles et si les vulnérabilités se trouvent dans des actifs de TI connectés à Internet. Il faut également indiquer si des mesures d'atténuation ou des contrôles compensatoires ont déjà été mis en œuvre pour chaque facteur.
- **Grande valeur ajoutée à la détermination des risques :** les facteurs de risque devraient ajouter une grande valeur à la détermination des risques.
- **Guide d'évaluation non ambigu :** un guide d'évaluation devrait expliquer dans un langage non ambigu la façon dont les différentes cotes sont évaluées pour chaque facteur de risque.
- **Mécanisme d'évaluation transparent :** le guide d'évaluation devrait également expliquer comment les cotes de chaque facteur de risque sont combinées pour en arriver à une cote de risque globale. Ce processus devrait être transparent, simple et facile à comprendre.

Une méthode d'évaluation des risques liés aux vulnérabilités devrait produire deux éléments d'analyse essentiels.

1. **Cote de risque globale :** indique le niveau de risque associé à un actif vulnérable.
2. **Échéances d'atténuation :** échéances précises d'atténuation liées aux cotes de risque, qui diminuent à mesure que le risque augmente. Ces échéances devraient correspondre à celles d'organisations semblables et être efficaces contre les vitesses d'exploitation connues des auteurs

de menace, comme rapportées par les fournisseurs et les sources de renseignements.

Il existe de nombreuses façons d'effectuer une évaluation des risques. Par exemple, la Cybersecurity and Infrastructure Security Agency (CISA) a publié la catégorisation des vulnérabilités propres aux intervenants (en anglais), qui constitue un exemple d'utilisation d'arbres décisionnels. Le calcul du risque moyen pondéré est une autre méthode d'évaluation. L'annexe C présente une approche d'évaluation des risques liés aux vulnérabilités fondée sur une cote de risque moyenne pondérée tenant compte des facteurs de risque suivants :

- cote de risque du fournisseur;
- cote technique liée aux vulnérabilités;
- maturité de l'exploitation;
- importance des actifs pour les auteurs de menace;
- importance des actifs pour les activités opérationnelles;
- exposition externe de l'actif.

Bien qu'il soit essentiel de respecter les échéances d'atténuation, des exceptions et des exemptions peuvent s'appliquer à la mise en œuvre de correctifs. Par rapport aux vulnérabilités pour lesquelles il n'existe aucun correctif, d'autres mesures d'atténuation (par exemple, la segmentation du réseau) ou des solutions de rechange temporaires (par exemple, désactiver la fonction vulnérable) peuvent servir de mesures provisoires. Quand il ne s'agit pas d'une vulnérabilité du jour zéro, d'autres mesures d'atténuation peuvent également être acceptables, mais elles ne doivent pas exposer l'organisation à des risques supplémentaires. Toute exception aux échéances d'atténuation établies doit être appuyée par une évaluation des risques confirmant que les mesures de rechange atténuent adéquatement le risque.

Dans certains cas, les responsables du risque peuvent décider d'accepter certains risques associés aux vulnérabilités. Un processus officiel d'acceptation des risques et un registre d'acceptation des risques sont cruciaux pour gérer les vulnérabilités qui ne peuvent être immédiatement atténuées. Ce processus consiste à documenter les cas où une organisation décide d'accepter les risques associés à une vulnérabilité donnée plutôt que d'immédiatement mettre en œuvre des mesures correctives. Le registre d'acceptation des risques doit contenir :

- la justification pour chaque décision d'acceptation, y compris une analyse de l'incidence par rapport au coût des mesures d'atténuation et s'il existe des mesures de contrôle en place qui atténuent partiellement le risque;
- les conditions dans lesquelles l'acceptation du risque sera examinée et potentiellement revue, comme les changements dans le contexte des menaces ou l'existence de stratégies d'atténuation plus efficaces.

Ce registre constitue un outil essentiel pour faire le suivi des risques acceptés au fil du temps, en veillant à ce qu'ils soient connus, justifiés et continuellement évalués par rapport à la situation de sécurité et à la tolérance au risque de l'organisation. Toute acceptation de risque doit inclure une date d'expiration de moins de 12 mois à compter de la date d'acceptation. Ce délai permet de nouvelles acceptations et des examens réguliers.

2.5 Activités d'atténuation

L'atténuation des vulnérabilités peut prendre plusieurs formes, selon la nature et la gravité des vulnérabilités, la complexité et le caractère essentiel du système vulnérable, et même l'existence d'un correctif. Bien que cela ne

soit pas toujours possible, la méthode privilégiée consiste à mettre en œuvre le correctif fourni par le fournisseur ou à ajuster les paramètres de configuration pour corriger entièrement le problème.

2.5.1 Correctifs

Les correctifs sont des mises à jour apportées aux micrologiciels et aux logiciels pour corriger des lacunes fonctionnelles et de sécurité. Il est essentiel d'appliquer des correctifs aux systèmes d'exploitation, aux applications et aux dispositifs pour assurer leur sécurité. En tirant parti de l'automatisation pour faciliter la mise en œuvre des correctifs, on peut améliorer considérablement l'efficacité et la précision, réduire le risque d'erreur humaine et veiller à l'installation rapide des mises à jour essentielles. Les correctifs d'urgence, souvent mis en œuvre en réponse à des vulnérabilités du jour zéro, devraient suivre un calendrier de changements d'urgence bien défini.

Les correctifs et les mises à jour doivent faire l'objet d'un suivi au moyen du système ministériel de gestion des changements (Directive sur la gestion de la sécurité, sous-section B.2.3.3). Les plans de mise en œuvre des correctifs doivent inclure des mesures d'urgence et de retour en arrière. Le document Correction des systèmes d'exploitation et des applications – Bulletin de sécurité des TI à l'intention du gouvernement du Canada (ITSM-96) contient des renseignements plus détaillés sur la gestion des correctifs.

2.5.2 Changements de configuration

Les changements de configuration constituent une mesure commune et essentielle d'atténuation des vulnérabilités et devraient être inclus dans les processus de gestion de la configuration et du changement. Les changements de configuration comprennent la modification des

paramètres du système pour accroître la sécurité et atténuer les vulnérabilités. On parle alors communément d'une configuration renforcée, selon Les 10 mesures de sécurité des TI visant à protéger les réseaux Internet et l'information (ITSM.10.089) du Centre canadien pour la cybersécurité. Les fonctions généralement activées par défaut doivent être désactivées pour limiter le plus possible l'exposition et éviter de mettre en œuvre des correctifs d'urgence s'ils ne sont pas nécessaires. Le renforcement peut également comprendre la désactivation ou la suppression de comptes et de services non requis, la modification des mots de passe par défaut du fabricant, et la modification des contrôles d'accès. Les changements de configuration devraient être consignés et gérés au moyen du processus de gestion de la configuration afin qu'ils soient mis en œuvre de façon correcte et uniforme. Des examens et des audits réguliers des configurations peuvent aider à maintenir la sécurité et la conformité.

2.5.3 Contrôles compensatoires

L'atténuation complète est l'option privilégiée pour corriger les vulnérabilités. Lorsque les correctifs ou les changements de configuration ne peuvent pas être immédiatement mis en œuvre, les contrôles compensatoires offrent d'autres moyens de maintenir la sécurité et de réduire les risques. L'objectif des contrôles compensatoires est de permettre la continuité des activités tout en s'attaquant aux enjeux de sécurité. Souvent, de multiples contrôles compensatoires sont combinés pour ramener le risque à un niveau acceptable jusqu'à ce qu'il soit possible de mettre en œuvre une solution permanente.

Voici des exemples de contrôles compensatoires (liste non exhaustive).

- **Zonage de sécurité du réseau :** segmenter le réseau pour isoler les systèmes vulnérables et limiter les vecteurs d'attaque potentiels.

- **Pare-feu d'applications Web :** protéger les applications Web par le filtrage et la surveillance du trafic HTTP entre les applications Web et Internet.
- **Systèmes de détection et de prévention des intrusions :** surveiller les activités des réseaux ou des systèmes pour déceler des activités malveillantes ou des violations des politiques et prendre des mesures préventives
- **Désactivation ou suppression de services ou de logiciels vulnérables :** désactiver ou désinstaller temporairement des services ou des logiciels dont la vulnérabilité est connue.
- **Contrôles d'accès :** mettre en œuvre des contrôles d'accès stricts pour limiter les personnes pouvant accéder aux systèmes et aux données sensibles.
- **Liste d'applications autorisées :** ne permettre que l'exécution d'applications autorisées sur le réseau afin de réduire le risque d'exécution de logiciels malveillants.
- **Formation sur la sensibilisation à la sécurité :** sensibiliser les employés aux pratiques exemplaires en matière de sécurité et à la façon de reconnaître les menaces potentielles.
- **Surveillance accrue :** renforcer les activités de surveillance pour détecter les activités inhabituelles ou les tentatives d'exploitation et y réagir rapidement.

Les contrôles compensatoires doivent être revus et réapprouvés au moins une fois par année pour assurer leur efficacité et conformité continues face à l'évolution des menaces.

2.5.4 Soutien culturel pour l'atténuation

Les activités d'atténuation efficaces reposent sur une culture organisationnelle de soutien. Un engagement ferme de la part des dirigeants permet d'accorder la priorité à la sécurité et de veiller à ce que

les ressources soient affectées de façon appropriée. Les dirigeants doivent participer activement aux discussions sur la sécurité et tenir les équipes responsables du rendement en matière de sécurité.

La collaboration entre les équipes des TI, de la sécurité, du développement et des autres ministères est essentielle. La tenue de réunions régulières pour discuter des exigences en matière de sécurité et coordonner les mesures de correction favorise une approche unifiée. Une culture axée sur la sécurité encourage les employés à suivre les pratiques exemplaires et à assumer leurs responsabilités en matière de sécurité. La formation sur la sensibilisation à la sécurité et la promotion du signalement des incidents constituent des éléments clés.

La communication ouverte et la transparence par rapport aux questions de sécurité favorisent la confiance et la coopération au sein des équipes. Des mises à jour régulières sur les activités d'atténuation et des processus consignés avec clarté sont essentiels. Grâce à l'amélioration continue, les stratégies d'atténuation évoluent de manière à pouvoir s'attaquer aux nouvelles menaces. Il est essentiel d'examiner et de mettre à jour les processus, de tenir compte de la rétroaction et d'investir dans la formation de manière régulière.

2.6 Mesures, production de rapports et conformité

Un programme de GV devrait comprendre une surveillance et une amélioration continues pour maintenir la sécurité face aux menaces en constante évolution. Cette approche comprend l'utilisation d'outils et de techniques pour surveiller les systèmes, effectuer des évaluations régulières et mettre en œuvre des mises à jour et des correctifs en temps opportun. Les mesures doivent évaluer la couverture, l'efficacité, l'efficience et la conformité des activités de GV. La production de rapports réguliers sur les mesures permettra à l'organisation d'établir un point de

référence en matière de rendement. Les mesures devraient être fondées sur des outils de gestion des services de TI afin que les vulnérabilités soient signalées et fassent l'objet d'un suivi aux fins d'atténuation. De plus, les mesures devraient être liées à un modèle de maturité de la GV afin de permettre une approche rationnelle et transparente de mesure la maturité du programme de GV. Les gestionnaires de programme peuvent utiliser les modèles de maturité pour cerner les domaines où le rendement souhaité est obtenu et ceux qui nécessitent des réformes et des investissements supplémentaires.

Les rapports et les tableaux de bord permettent d'assurer de manière continue la surveillance et l'évaluation de la conformité. Ces outils donnent à tout moment un aperçu de la situation de sécurité de l'organisation, ce qui permet de réagir rapidement aux nouvelles vulnérabilités et de respecter les exigences réglementaires.

Tableau 2.2 : Exemples de mesures de gestion des vulnérabilités

Catégorie	Mesure
Couverture	• **Couverture du répertoire :** pourcentage du matériel et des logiciels de l'organisation qui sont régulièrement inventoriés et évalués pour déceler des vulnérabilités.

Catégorie	Mesure
Efficience et efficacité	• **Mesures du temps requis pour mettre en œuvre les correctifs :** le temps minimal, moyen et maximal pour corriger un pourcentage donné d'hôtes. • **Temps moyen de correction :** le temps moyen s'écoulant entre la détection d'une vulnérabilité et sa correction, catégorisé par niveau de risque. • **Méthode de distribution du correctif :** le pourcentage d'hôtes qui ont fait l'objet d'un correctif automatique, partiel (dans le cas des correctifs regroupés dans un ensemble), et manuel.
Conformité	• **Conformité des mesures d'atténuation :** vulnérabilités dont la correction a pris plus de temps que la période d'atténuation requise. • **Exceptions et exemptions à la mise en œuvre de correctifs :** le nombre d'exceptions et d'exemptions appliquées à la mise en œuvre de correctifs.

L'Annexe D présente des mesures supplémentaires suggérées pour les programmes ministériels de GV.

2.7 Processus habilitants

La GV ne fonctionne pas en vase clos; elle repose sur un ensemble de processus de base qui fournissent une infrastructure et un soutien essentiels. Ces processus habilitants sont essentiels pour veiller à ce que les vulnérabilités soient détectées, évaluées et atténuées de façon systématique et efficace. Ils créent un cadre rigoureux qui améliore la situation de sécurité globale de l'organisation en intégrant divers aspects de la gestion des TI et de la sécurité.

La Stratégie intégrée de cybersécurité du GC – Annexe A MOSC décrit certains processus habilitants clés appuyant un programme de GV réussi. Elle souligne leurs objectifs et la façon dont ils contribuent à la détection, à l'ordre de priorité et à la correction des vulnérabilités. En comprenant et en mettant en œuvre ces processus, les organisations peuvent élaborer une approche complète et durable pour gérer les vulnérabilités et protéger leurs actifs.

- **Gestion du changement :** la gestion du changement permet la gestion systématique de tous les changements apportés aux systèmes de TI grâce à la mise en œuvre de politiques et d'outils permettant de faire le suivi des changements et de les consigner.
- **Gestion des correctifs :** la gestion des correctifs permet de corriger les vulnérabilités logicielles et matérielles au moyen de correctifs opportuns qui sont régulièrement revus et mis en œuvre au moyen d'outils automatisés.
- **Gestion de la configuration :** la gestion de la configuration permet d'assurer la sécurité des configurations des systèmes de TI au moyen d'outils permettant d'appliquer les paramètres sécurisés et de mettre régulièrement à jour les configurations.
- **Gestion des accès :** la gestion des accès permet de contrôler l'accès aux systèmes de TI. Elle empêche tout accès non autorisé au moyen de l'authentification multifacteur et de contrôles d'accès fondés sur les rôles.
- **Renseignements sur les menaces :** les renseignements sur les menaces permettent de rester au courant des nouvelles menaces et vulnérabilités grâce à l'intégration des sources de renseignements sur les menaces et à l'examen régulier des rapports.
- **Gestion des fournisseurs :** la gestion des fournisseurs garantit la conformité des fournisseurs tiers aux normes de sécurité grâce aux

évaluations régulières de sécurité et à l'ajout d'exigences en matière de sécurité dans les contrats.
- **Audits et conformité :** les audits et la conformité permettent d'assurer la conformité de l'organisation aux règlements et aux normes en matière de sécurité grâce à la réalisation d'audits réguliers et à la correction des lacunes en matière de conformité.
- **Activités de sensibilisation et de formation :** les activités de sensibilisation et de formation permettent de sensibiliser les employés à la GV et aux pratiques exemplaires en matière de sécurité grâce à l'élaboration d'un programme de formation, à la tenue de séances régulières et à l'offre de formation propre aux postes.

Pour obtenir de plus amples renseignements, consultez la Stratégie intégrée de cybersécurité du GC – Annexe A MOSC.

2.8 Considérations technologiques

Pour obtenir des renseignements détaillés sur les options technologiques et les capacités des plateformes d'identification des vulnérabilités, consultez le document sur l'amélioration des correctifs d'entreprise pour les systèmes de TI généraux : mieux utiliser les processus et les outils existants (NIST SP 1800-31) (en anglais), 1800-31B (avril 2022).

3. Conclusion

Un programme de GV réussi est essentiel pour protéger les actifs de TI d'une organisation et assurer la continuité des activités opérationnelles. Le présent document d'orientation vise à aider les organisations à mettre en œuvre un programme de gestion des vulnérabilités rigoureux et complet. Il décrit les éléments clés de la gouvernance en matière de GV, y compris les protocoles de prise de décisions, les stratégies d'évaluation et

d’atténuation des risques, les mesures du rendement, les exigences en matière de conformité et les ententes de niveau de service. Il souligne également l’importance que l’engagement des dirigeants, la collaboration interfonctionnelle et une culture axée sur la sécurité ont à titre d’éléments essentiels à l’efficacité du programme de GV.

Annexe A : Définitions

gestion de la surface d’attaque

La gestion de la surface d’attaque est le processus qui consiste à cerner, à répertorier et à sécuriser de manière continue tous les éléments numériques, les services et les points terminaux d’une organisation qui pourraient être exposés à des attaquants. L’objectif est de dresser systématiquement un répertoire et de réduire la vulnérabilité des points susceptibles d’être attaqués au sein de l’infrastructure numérique d’une organisation afin d’atténuer le risque de cybermenaces.

processus coordonné de divulgation des vulnérabilités

Le processus coordonné de divulgation des vulnérabilités comprend la gestion systématique des signalements, de l’analyse et de l’atténuation des vulnérabilités en matière de cybersécurité. L’objectif est de veiller à ce que les vulnérabilités relevées par les chercheurs, les utilisateurs ou d’autres intervenants soient directement signalées à l’organisation afin de permettre l’élaboration et le déploiement des correctifs ou des mesures d’atténuation nécessaires avant la divulgation publique. Ce processus aide à établir un équilibre entre la nécessité de divulguer rapidement les vulnérabilités et l’impératif de protéger les utilisateurs en réglant les problèmes avant qu’ils ne soient largement connus.

systèmes et services essentiels

Les systèmes et services essentiels sont définis par le Secrétariat du Conseil du Trésor comme ceux dont la compromission sur le plan de l’accessibilité ou de l’intégrité « porterait un préjudice élevé ou très élevé à la santé, à la

sûreté, à la sécurité ou au bien-être économique des Canadiens et des Canadiennes, ou encore au fonctionnement efficace du gouvernement du Canada ». (Source : Politique sur la sécurité du gouvernement.)

gestion des correctifs

Il s'agit d'un processus de gestion d'un réseau d'ordinateurs dans le cadre duquel des mises à jour et des correctifs sont régulièrement mis en œuvre pour assurer la protection des systèmes contre les vulnérabilités et les menaces à la sécurité [3].

essais de pénétration

Les essais de pénétration, ou tests d'intrusion, sont une cyberattaque simulée contre un système pour vérifier s'il existe des vulnérabilités exploitables. Il s'agit d'une tentative proactive et autorisée d'évaluer la sécurité d'un système en tentant d'exploiter ses vulnérabilités de façon sécuritaire.

nomenclature logicielle

Une nomenclature logicielle est un document officiel décrivant en détail les composantes et les relations de la chaîne d'approvisionnement des divers éléments utilisés pour créer un progiciel. Elle fonctionne comme un répertoire intégré qui dresse la liste de tous les éléments dont la solution logicielle complète se compose. Une nomenclature logicielle assure la transparence de la composition du logiciel et aide les organisations à détecter et à gérer les vulnérabilités, à assurer la conformité et à accroître la sécurité tout au long du cycle de vie du développement logiciel.

analyses de réseau

Les analyses de réseau comprennent l'utilisation d'outils logiciels pour repérer les dispositifs, serveurs et autres entités sur un réseau ainsi que leurs services, configurations et vulnérabilités. Il s'agit d'une étape essentielle dans l'évaluation de la situation de sécurité des réseaux.

renseignements sur les menaces

Il s'agit des renseignements sur les menaces et les auteurs de menace qui aident à atténuer les événements néfastes dans le cyberespace. Ils

comprennent les renseignements sur les mécanismes, les indicateurs, et les répercussions ainsi que les conseils pratiques au sujet des menaces existantes ou nouvelles.

vulnérabilité
Une vulnérabilité est une faiblesse ou une faille d'un système d'information, de procédures de sécurité des systèmes, de contrôles internes ou de mise en œuvre qui pourrait être exploitée par un auteur de menace pour obtenir un accès non autorisé à l'information ou perturber les services essentiels. Les vulnérabilités peuvent provenir de diverses sources, y compris de bogues logiciels, d'erreurs de configuration ou de pratiques de sécurité inadéquates.

Annexe B : Liste de contrôle pour la gestion des vulnérabilités

▼ Dans cette section

Voici une liste de contrôle qui résume les principaux éléments abordés dans le présent document. Cette structure aide à établir un programme clair et efficace de gestion des vulnérabilités qui cadre avec les objectifs

organisationnels et assure la protection des actifs essentiels.

B-1 : Liste de contrôle pour la gestion des vulnérabilités

1. Gouvernance

Objectif : établir une structure officielle pour gérer les vulnérabilités et assurer la responsabilisation.

Étapes

- Définir la portée et les objectifs du programme.
- Attribuer les rôles et les responsabilités (par exemple, équipe de la sécurité, propriétaires d'actif, cadres responsables).
- Élaborer des politiques et des procédures pour orienter les activités de gestion des vulnérabilités.
- Veiller au respect des politiques, des normes et des exigences réglementaires du GC.

2. Compréhension des dépendances opérationnelles des actifs de TI

Objectif : cerner les actifs essentiels et leurs dépendances.

Étapes

- Faire l'inventaire de tous les actifs de TI, y compris le matériel, les logiciels et les composants de réseau.
- Procéder au mappage entre les processus opérationnels et les actifs de TI dont ils dépendent.
- Établir l'ordre de priorité des actifs en fonction de leur importance pour les activités opérationnelles et de la sensibilité des données.

3. Détection des vulnérabilités

Objectif : détecter les vulnérabilités des actifs de TI afin de gérer les risques de façon proactive.

Étapes

- Effectuer régulièrement des évaluations internes et externes à l'aide d'outils automatisés.
- Compléter les évaluations automatisées par de la validation et des tests manuels.
- Tirer parti des résultats des interventions en cas d'incident pour cerner les lacunes.
- Surveiller les sources de renseignements sur les menaces pour trouver les vulnérabilités nouvellement divulguées.

4. Évaluation des risques liés aux vulnérabilités

Objectif : évaluer les vulnérabilités et établir leur ordre de priorité en fonction de leur incidence potentielle et de leur probabilité.

Étapes

- Évaluer la gravité des vulnérabilités détectées.
- Tenir compte de l'importance de l'actif et de son exposition aux menaces.
- Créer une matrice de risques pour catégoriser les vulnérabilités en fonction de leur priorité (par exemple, risque élevé, moyen ou faible).

5. Activités d'atténuation

Objectif : corriger les vulnérabilités ou mettre en place des contrôles compensatoires pour réduire les risques jusqu'à ce que les vulnérabilités soient entièrement corrigées.

Étapes

- Mettre en œuvre un correctif ou une mise à jour dans les systèmes et applications concernés.
- Apporter des changements à la configuration pour atténuer temporairement les risques.
- Mettre en œuvre des contrôles compensatoires pour réduire les risques à un niveau acceptable lorsqu'une correction complète n'est pas possible ou prendrait trop de temps.

6. Mesures, production de rapports et conformité

Objectif : mesurer l'efficacité du programme et démontrer la conformité.

Étapes

- Élaborer des indicateurs de rendement clés (par exemple, temps de correction, nombre de vulnérabilités à risque élevé corrigées).
- Produire des rapports réguliers pour les intervenants qui présentent les tendances et les réalisations.
- Assurer l'harmonisation avec les exigences réglementaires et d'audit au moyen de preuves écrites.

B-2 : Listes de contrôle détaillées sur le programme

Cette section fournit des listes de contrôle supplémentaires pour assurer l'exécution efficace du programme et son amélioration continue. Ces listes de contrôle portent sur la gouvernance, l'exécution opérationnelle et l'intégration aux fonctions élargies de sécurité des TI. Les ministères peuvent les utiliser pour évaluer eux-mêmes la maturité de leur programme de GV et sa conformité avec les Lignes directrices sur la gestion des vulnérabilités.

Tableau B.1 : Liste de contrôle sur les fondements des politiques et de la gouvernance

Élément de la liste de contrôle	État (Oui / Non / S. O.)	Remarques
Le ministère a une politique officielle en matière de gestion des vulnérabilités.		
La politique est approuvée par la haute direction.		
La structure de gouvernance est consignée (rôles, voies hiérarchiques, pouvoirs décisionnels).		
La politique sur la GV est harmonisée avec les instruments de politique du GC (par exemple, ITSG-33, PGEC GC, politiques liées à la cybersécurité du GC).		
Les rôles et les responsabilités sont définis pour les intervenants responsables des TI, de la sécurité et des activités opérationnelles.		
La GV fait partie du mandat des organes de gouvernance ou des comités directeurs ministériels en matière de cybersécurité.		

Tableau B.2 : Liste de contrôle sur l’inventaire des actifs et le mappage selon l’importance

Élément de la liste de contrôle	État (Oui / Non / S. O.)	Remarques

Il existe un inventaire des actifs des TI à jour et faisant autorité (matériel, logiciel et systèmes).		
L'inventaire comprend le propriétaire du système, l'environnement, les fonctions opérationnelles et le niveau de sensibilité.		
Les actifs sont classés selon l'importance (par exemple, essentiels à la mission, internes ou accessibles au public).		
Les systèmes et les services qui sont exposés à l'externe sont clairement identifiés et font l'objet d'un suivi.		
Les responsables du programme de GV ont accès aux données sur les actifs pour établir la portée et l'ordre des priorités.		
Les capteurs au niveau de l'hôte du CCCS sont déployés sur tous les points terminaux clients et les capteurs infonuagiques sont mis en œuvre conformément aux mesures de protection du nuage du GC.		

Tableau B.3 : Liste de contrôle sur la détection et la surveillance des vulnérabilités

Élément de la liste de contrôle	**État** (Oui / Non / S. O.)	**Remarques**

Les analyses internes sont effectuées au moins une fois par semaine (ou selon un calendrier établi).		
Les analyses externes sont effectuées au moins une fois par mois.		
Les analyses portent sur l’ensemble de l’inventaire des actifs autorisés.		
Les résultats des analyses sont ajoutés à l’inventaire des actifs, aux systèmes de gestion des billets ou aux plateformes de GIES.		
Les attaques du jour zéro et les menaces émergentes font l’objet d’un suivi sur les sites des fournisseurs, la liste des vulnérabilités exploitées connues de la CISA, le système de cote de prédiction des exploitations et les alertes du CCCS.		
Le processus coordonné de divulgation des vulnérabilités est établi et surveillé.		

Tableau B.4 : Liste de contrôle sur la priorisation et l’évaluation des risques

Élément de la liste de contrôle	**État** (Oui / Non / S. O.)	**Remarques**
Une méthodologie documentée d’évaluation des risques est utilisée (par exemple, la moyenne pondérée ou l’arbre de décision).		

Des facteurs comme le Système commun de notation des vulnérabilités, l'exploitabilité, l'importance de l'actif et l'exposition sont pris en considération.		
La liste des vulnérabilités exploitées connues de la CISA, le système de cote de prédiction des exploitations ou les renseignements sur les menaces étoffent les évaluations des risques.		
Les vulnérabilités à risque élevé sont identifiées, font l'objet d'un suivi et sont transmises aux échelons supérieurs, conformément aux politiques.		
Les seuils de tolérance aux risques et la logique décisionnelle sont consignés et revus régulièrement.		

Tableau B.5 : Liste de contrôle sur la correction et le traitement des risques

Élément de la liste de contrôle	État (Oui / Non / S. O.)	Remarques
Les délais de correction sont documentés (par exemple, 2, 14, 60 ou 90 jours selon le niveau de risque).		
Les objectifs des ententes de niveau de service font l'objet d'un suivi et de rapports.		
L'acceptation des risques est officiellement consignée et approuvée par la direction.		

Lorsque des corrections ne peuvent être apportées, les contrôles compensatoires sont évalués et documentés.		
Les processus de gestion du changement permettent d’effectuer des correctifs et des corrections en cas d’urgence.		

Tableau B.6 : Liste de contrôle de vérification et de validation

Élément de la liste de contrôle	État (Oui / Non / S. O.)	Remarques
Une nouvelle analyse est effectuée après la correction afin de vérifier que la vulnérabilité a été corrigée.		
La validation comprend des essais fonctionnels des correctifs ou des mesures d’atténuation.		
Des preuves de correction et de validation sont conservées (par exemple, journaux, billets, captures d’écran).		
Les vulnérabilités corrigées sont consignées dans les systèmes de gestion des billets ou de rapports.		

Tableau B.7 : Liste de contrôle sur les mesures et les rapports

Élément de la liste de contrôle	État (Oui / Non / S. O.)	Remarques
Les mesures sont définies (par exemple, temps moyen de réparation, pourcentage de couverture, vulnérabilités non corrigées, respect des ententes de niveau de service).		
Les tableaux de bord ou les rapports réguliers sont transmis aux principaux intervenants (par exemple, responsables des activités des TI, direction).		
Les mesures sont présentées aux comités de gouvernance en matière de cybersécurité.		
Les tendances, les lacunes et les problèmes systémiques sont définis à l'aide des mesures et orientent les mises à jour du programme.		

Tableau B.8 : Liste de contrôle sur l'intégration des interventions en cas d'incident et les processus liés à la sécurité des TI

Élément de la liste de contrôle	État (Oui / Non / S. O.)	Remarques
Le processus de GV est intégré au plan d'intervention en cas d'incident.		

Les renseignements sur les menaces du CCCS (par exemple, alertes Cyber Flash) et les directives du SCT (par exemple, demandes d'action) font partie du processus de GV.		
Le ministère est abonné au Système national de notification des cybermenaces (SNNCM) du CCCS.		
Les vulnérabilités à risque élevé peuvent déclencher des mesures d'intervention en cas d'incident (par exemple, recherches sur les indicateurs de compromission, repérages des menaces).		
Les rôles et les communications concernant les activités d'exploitation sont consignés.		
Les résultats sur les vulnérabilités orientent la modélisation des menaces, les évaluations de contrôle et les examens des projets de TI.		
Le plan de gestion des événements de cybersécurité du ministère comprend des renvois aux intrants et aux actions liées à la GV.		

Tableau B.9 : Liste de contrôle sur l'amélioration continue et l'état de préparation aux audits

Élément de la liste de contrôle	État (Oui / Non / S. O.)	Remarques
Les plans et les politiques liés à la GV sont examinés annuellement ou après des événements majeurs.		

Les leçons apprises des incidents ou des audits sont consignées et servent à apporter des améliorations.		
Des examens du programme de GV sont menés périodiquement à l'interne (par exemple, évaluation d'un cadre de maturité lié à la GV) ou par un tiers.		
Les intervenants de la GV reçoivent une formation adaptée à leurs rôles (par exemple, analystes, propriétaires de systèmes).		
Les mises à jour du programme sont fondées sur les technologies émergentes, les orientations du GC et les incidents réels.		

Annexe C : Outil d'évaluation des risques liés aux vulnérabilités

▼ Dans cette section

L'objectif de cet outil d'évaluation des risques liés aux vulnérabilités est :

- de disposer d'une approche rationnelle, justifiable et facile à utiliser pour établir l'ordre de priorité des vulnérabilités en fonction du risque qu'elles représentent pour la prestation de services essentiels et la situation de l'organisation en matière de cybersécurité;

- de définir des attentes en matière de correction des vulnérabilités qui concordent avec celles d'organisations semblables et tiennent compte de la vitesse de développement d'exploitations des auteurs de menace;
- d'adopter une approche uniforme à l'échelle du GC.

L'outil d'évaluation des risques liés aux vulnérabilités adopte les pratiques exemplaires de l'industrie. En règle générale, les organisations du GC devraient accorder la priorité aux **systèmes et services essentiels** dans tout scénario d'atténuation. Le risque potentiel plus élevé pour ces systèmes devrait être pris en compte dans l'outil d'évaluation des risques liés aux vulnérabilités. Une bonne compréhension et un répertoire complet des systèmes essentiels sont également importants pour la continuité des activités et la reprise après un sinistre de TI.

C-1 : processus

Les étapes suivantes doivent être suivies lors de l'utilisation de l'outil.

1. Évaluer chaque facteur de risque.
2. Additionner les notes (total de 50 points).
3. Déterminer où la note se situe dans la matrice de risques pour les délais de mise à l'essai et de correction.

Les éléments suivants doivent être pris en compte lors de l'utilisation de l'outil.

- Une expertise spécialisée est requise pour évaluer les facteurs.
- Si un facteur ne peut pas être évalué, il faut calculer la somme des autres notes en tant que pourcentage de points disponibles et catégoriser comme suit :
    - rouge = 80 % à 100 %;
    - orange = 60 % à 79 %;
    - jaune = 40 % à 59 %;

- vert = 1 % à 39 %.

C-2 : facteurs de risque

Le tableau C.1 présente les facteurs de risque.

Tableau C.1 : Tableau des facteurs de risque (total de 50 points)

Facteur	Description	Note maximale
Cote de risque du fournisseur	Fournie par le fournisseur	5
Exploitabilité technique et incidence technique (cote de base du Système commun de notation des vulnérabilités)	Fourni dans la National Vulnerability Database	10
Maturité de l'exploitation	Mesure dans laquelle l'exploitation est accessible et utilisée sur des réseaux	10
Importance des actifs pour les activités de menace	Importance de l'actif vulnérable pour les auteurs de menace en raison de ce que l'actif permettrait d'accomplir	5
Importance des actifs pour les activités opérationnelles	Importance de l'actif vulnérable pour les activités selon les activités, l'application ou le registre des risques du système	10
Exposition externe de l'actif	Mesure dans laquelle l'actif vulnérable est accessible par Internet	10

C-3 : guides d’évaluation des facteurs de risque

La section suivante présente des guides d’évaluation pour plusieurs facteurs de risque. Comme indiqué dans le tableau C.1, la cote de risque du fournisseur et la cote de base du Système commun de notation des vulnérabilités sont fournies par le fournisseur et la National Vulnerability Database.

Tableau C.2 : Guide d’évaluation de la maturité des exploitations

Points	Description
De 8 à 10	Un code autonome fonctionnel existe ou aucune exploitation n’est requise (déclenchement manuel) et l’information est largement accessible. Le code d’exploitation fonctionne dans toutes les situations ou est activement livré par l’intermédiaire d’un agent autonome (comme un ver ou un virus). Les systèmes connectés au réseau pourraient subir des tentatives d’analyse ou d’exploitation. Le développement de l’exploitation a atteint le niveau d’outils automatisés fiables, largement accessibles et faciles à utiliser.
De 5 à 7	Le code d’exploitation fonctionnel est accessible. Le code fonctionne dans la plupart des situations où il existe une vulnérabilité.
De 3 à 4	Un code d’exploitation de validation de principe est accessible, ou une démonstration d’attaque n’est pas pratique pour la plupart des systèmes. La technique ou le code n’est pas fonctionnel dans toutes les situations et pourrait nécessiter des modifications importantes de la part d’un attaquant compétent.
De 1 à 2	Aucun code d’exploitation n’est accessible, ou l’exploitation est théorique.

Tableau C.3 : Guide d’évaluation de l’importance des actifs pour les activités de menace

Points	Description

De 4 à 5	• L’actif contient des renseignements de nature délicate qui peuvent entraîner un vol de données (par exemple, failles d’injection de base de données, stockage de données non chiffrées, interface de programmation d’application [API] exposée).
	• L’actif héberge des services intégrés où un manque de disponibilité a des effets accessoires (par exemple, service temps, service de nom de domaine [DNS], services fédérés, autorité de certification).
	• L’actif fournit un accès initial à un attaquant, ce qui entraîne un potentiel d’intrusion (par exemple, services à distance exposés, applications Web accessibles au public non sécurisées, ports ouverts, vulnérabilités du réseau privé virtuel [RPV]).
	• L’actif contient un stockage d’identité qui permet à un attaquant de transmettre les privilèges à un niveau supérieur par un :
	  ◦ ocontrôle des comptes, qui permet d’accéder à l’infrastructure réseau ou aux points terminaux avec des privilèges d’administrateur;
	  ◦ ocontrôle des comptes utilisés pour accéder à des données sensibles;
	  ◦ ocontrôle des comptes de service;
	  ◦ ocontrôle des comptes utilisés pour les requêtes API;
	  ◦ ocontrôle des comptes permettant l’accès à l’environnement réseau.

Points	Description
3	• L’actif permet à un attaquant d’accéder, sans authentification, aux ressources locales disposant de privilèges d’utilisateur.
De 1 à 2	• L’actif permet aux attaquants de passer d’un actif à l’autre en étendant leur influence (par exemple, failles de protocole réseau, applications Web internes non sécurisées, comptes de service non sécurisés). • L’actif peut être exploité par les attaquants pour conserver un accès au fil du temps (par exemple, sauvegardes régulières non sécurisées, micrologiciels vulnérables, vulnérabilités d’exécution automatique).

Tableau C.4 : Guide d’évaluation de l’importance des actifs pour les activités opérationnelles

Points	Description
De 8 à 10	L’actif est essentiel aux principales activités opérationnelles. La compromission de cet actif a une incidence directe sur la continuité des activités et pourrait avoir de graves répercussions financières, opérationnelles ou sur la réputation. Un nombre plus élevé d’actifs touchés correspond généralement à une cote plus élevée. Peut comprendre les actifs prenant en charge les systèmes Protégé B. Comprend les actifs prenant en charge l’information catégorisée comme Secret et Protégé C.
De 5 à 7	L’actif appuie les activités opérationnelles essentielles, mais n’en est pas le moteur principal. La compromission de l’actif n’interrompra pas les activités opérationnelles, mais pourrait causer des perturbations ou inconvénients importants.

Points	Description
De 3 à 4	L’actif prend en charge des fonctions opérationnelles secondaires qui ne sont pas étroitement liées aux activités principales. Sa compromission, bien que nuisible, peut être gérée sans perturbation importante aux principales fonctions.
De 1 à 2	L’actif appuie des tâches ou des opérations non essentielles, et la compromission aurait une incidence minime. Sa compromission a une incidence immédiate minime sur les principales fonctions opérationnelles. L’actif peut servir à des rôles périphériques et non essentiels et peut être facilement remplacé ou omis.

Tableau C.5 : Guide d’évaluation de l’exposition externe des actifs

Points	Description
De 8 à 10	L’actif vulnérable est routable de l’extérieur. Un auteur de menace pourrait exploiter l’actif à partir d’Internet.
De 5 à 7	L’actif vulnérable est exploitable à distance. Un auteur de menace doit accéder au même réseau étendu (RE) que l’actif vulnérable pour l’exploiter.
De 3 à 4	L’actif vulnérable est exploitable à partir du réseau local. Un auteur de menace doit accéder au même segment de réseau que l’actif vulnérable pour l’exploiter.
2	L’actif vulnérable est exploitable localement. Un auteur de menace doit avoir un accès direct à l’actif vulnérable.
1	L’actif vulnérable est physiquement exploitable. Un auteur de menace doit avoir un accès physique à l’actif vulnérable.

C-4 : matrice de risques

Le tableau C.6 présente les délais recommandés pour la mise à l'essai et la correction des vulnérabilités détectées.

Tableau C.6 : Matrice de risques

Points	Pourcentage	Niveau de risque global	Délai de correction	Processus
De 40 à 50	De 80 % à 100 %	Critique	48 heures	Renvoi au PGEC GC; correction de la vulnérabilité ministérielle
De 30 à 39	De 60 % à 79 %	Élevé	14 jours	Correction de la vulnérabilité ministérielle
De 20 à 29	De 40 % à 59 %	Moyen	30 jours	Correction de la vulnérabilité ministérielle
De 1 à 19	De 1 % à 39 %	Faible	90 jours	Correction de la vulnérabilité ministérielle

Annexe D : Mesures supplémentaires

Pour gérer efficacement les vulnérabilités, il faut des mesures significatives et à plusieurs niveaux qui facilitent la prise de décisions des responsables techniques et du programme, ainsi que de la direction. Plutôt que de se

concentrer uniquement sur les chiffres bruts, les ministères devraient utiliser des mesures qui contextualisent l’exposition, hiérarchisent les risques et permettent d’observer les tendances au fil du temps.

Le tableau suivant présente les mesures suggérées, les méthodes de calcul, et la façon de les utiliser pour faciliter la compréhension et la responsabilisation. Les ministères devraient les adapter en fonction de leurs réalités opérationnelles, leurs structures hiérarchiques et leurs contextes opérationnels.

Tableau D.1 : Mesures

Catégorie	Sous-catégorie	Description

Mesures de base sur la gestion des vulnérabilités	*Sans objet*	• Nombre de serveurs analysés : nombre total de serveurs analysés par un outil de GV (avec ou sans authentifiants). • Couverture : pourcentage des actifs de TI inclus dans les analyses de vulnérabilités et la gestion des correctifs régulières (l'objectif est que 100 % des actifs visés soient couverts). • Nombre d'anciens serveurs vulnérables : serveurs équipés de systèmes d'exploitation en fin de vie. • Nombre de serveurs existants vulnérables : serveurs équipés de systèmes d'exploitation pris en charge par les fournisseurs. • Nombre de serveurs sans authentifiants analysés : données sur les vulnérabilités incomplètes. • Nombre de serveurs avec authentifiants analysés : objectif principal pour les corrections. • Nombre de serveurs sans plan de correction : exclus en raison des dépendances ou des mises hors service

		• Nombre de serveurs assortis d’un plan de correction : corrections actives • Nombre total de vulnérabilités détectées dans tous les serveurs analysés. • Nombre total de vulnérabilités détectées dans les anciens serveurs. • Nombre total de vulnérabilités détectées dans les serveurs existants. • Nombre total de vulnérabilités analysées avec authentifiants. • Nombre total de vulnérabilités assorties d’un plan de correction.

Mesures à plusieurs niveaux sur l’analyse des risques	*Sans objet*	Les mesures brutes, comme le nombre de vulnérabilités non corrigées, sont insuffisantes. Pour que les mesures soient exploitables et tiennent compte des risques, les ministères doivent envisager : • une normalisation en fonction du volume d’actifs (par exemple, vulnérabilités pour 100 actifs); • un filtrage selon l’importance de l’actif ou sa fonction opérationnelle; • une pondération basée sur l’exploitabilité (par exemple, liste des vulnérabilités exploitées connues, exploits actifs); • le retrait des exceptions acceptées du nombre total de mesures exploitables; • l’analyse des tendances pour déterminer les améliorations ou les régressions. Exemple de mesure composée : • la densité des vulnérabilités critiques ou des vulnérabilités exploitées connues sur les actifs ayant une incidence élevée (pour 100 actifs), en

		excluant les éléments reportés. Cette approche à plusieurs niveaux ne montre pas seulement l’arriéré technique, mais aussi les risques organisationnels.

Mesures opérationnelles	**Vulnérabilités non corrigées par date (répartition selon le niveau de gravité)**	**Justification :** Le suivi des vulnérabilités non corrigées par date permet de mettre en évidence les retards de correction, de cibler les problèmes systémiques liés à la gestion des correctifs et d'accorder la priorité aux vulnérabilités à risque élevé plus anciennes susceptibles d'exposer les systèmes du GC. Cette mesure favorise la production de rapports sur la conformité et le respect des ententes de niveaux de service. **Méthode de calcul :** écart entre la première et la dernière vulnérabilité détectée.
	Vulnérabilités non corrigées par anciens serveurs et serveurs existants	**Justification :** Souvent, les anciens systèmes ne sont pas pris en charge par les fournisseurs. Ces systèmes présentent donc un risque élevé et sont plus difficiles à corriger. Cette mesure permet de déterminer la dette technique et d'orienter les plans de migration et de mise hors service. **Méthode de calcul :** filtrer les résultats des analyses pour obtenir les serveurs dont le système d'exploitation est en fin de vie.

Actifs accessibles par Internet et actifs internes	**Justification :** Les actifs accessibles par Internet sont plus exposés et doivent être corrigés plus rapidement. Cette mesure vise à accorder la priorité aux risques et à faciliter la production de rapports sur la conformité. **Méthode de calcul :** • Actifs accessibles par Internet = nombre d’actifs ayant des adresses IP publiques ou des serveurs DNS accessibles de l’extérieur. • Actifs internes = nombre d’actifs dont l’accès est limité au réseau interne.

	Nombre total de vulnérabilités par composantes (système d’exploitation, application et configuration)	**Justification :** Cette mesure vise à déterminer quelle composante présente le risque le plus élevé (système d’exploitation, application, configuration). Elle permet d’établir des stratégies ciblées en matière de correction (par exemple, correctif du système d’exploitation, mise à jour ou renforcement de l’application). **Méthode de calcul :** classer chaque résultat par composante d’après les données d’analyse des vulnérabilités : • composante du système d’exploitation : vulnérabilités et expositions communes liées au système d’exploitation (par exemple, Windows, Linux); • composante de l’application : vulnérabilités et expositions communes liées aux applications installées (par exemple, navigateurs, outils de productivité); • composante de la configuration : erreurs de configuration ou paramètres du registre manquants.

	Vulnérabilités non corrigées par gravité (normalisées)	**Justification :** Les vulnérabilités exploitées connues posent le risque le plus élevé; les pirates informatiques les ciblent activement. Le fait d'accorder la priorité à ces vulnérabilités réduit la probabilité de compromission. **Méthode de calcul :** comparer les résultats de l'analyse avec la liste des vulnérabilités exploitées connues de la CISA (ou la liste des vulnérabilités du GC lorsqu'elle sera disponible).
	Vulnérabilités non corrigées par vulnérabilités exploitées connues (normalisées)	**Justification :** Cette mesure présente les vulnérabilités non corrigées pour 100 actifs analysés afin d'éviter de pénaliser des équipes ou des ministères de plus grande taille. **Méthode de calcul :** vulnérabilités exploitées connues non corrigées ÷ nombre total d'actifs analysés × 100
	Temps de correction	**Justification :** Cette mesure calcule le temps moyen ou médian requis pour corriger des vulnérabilités. **Méthode de calcul :** date de correction — date de détection (moyen/médian).

	Couverture des exploits accessibles	**Justification :** Cette mesure indique le nombre de vulnérabilités instrumentalisées connues qui restent à corriger. **Méthode de calcul :** Nombre de vulnérabilités et expositions communes récurrentes figurant sur la liste des vulnérabilités exploitées connues non corrigées ÷ nombre total de vulnérabilités et expositions communes récurrentes figurant sur la liste des vulnérabilités exploitées connues × 100
	Vulnérabilités récurrentes / Taux de récurrence	**Justification :** Cette mesure signale les lacunes en matière de correction ou de configuration lorsque des vulnérabilités réapparaissent. **Méthode de calcul :** nombre de vulnérabilités et expositions communes récurrentes ÷ nombre total de vulnérabilités et expositions communes corrigées au cours de la même période.

Mesures liées au programme	**Vulnérabilités non corrigées par équipe**	**Justification :** Cette mesure indique les équipes qui ont les plus importants arriérés concernant les vulnérabilités. Elle permet d'affecter les ressources et d'orienter les mesures correctives aux équipes qui en ont le plus besoin. **Méthode de calcul :** nombre de vulnérabilités non corrigées par équipe = SOMME (vulnérabilités non corrigées OÙ équipe assignée = X).
	Taux de conformité à l'entente de niveau de service	**Justification :** Cette mesure calcule la fréquence à laquelle les vulnérabilités sont corrigées dans les délais impartis. **Méthode de calcul :** nombre de vulnérabilités corrigées dans les délais impartis de l'entente de niveau de service ÷ nombre total de vulnérabilités corrigées × 100.
	Arriéré des vulnérabilités — Vulnérabilités non corrigées de plus de 90 jours	**Justification :** Cette mesure indique les violations aux ententes de niveau de service et les retards systémiques. **Méthode de calcul :** nombre de vulnérabilités de plus de 90 jours.

Suivi des exceptions et des exclusions	**Justification :** Cette mesure fait le suivi des risques non résolus qui ont été reportés ou acceptés. **Méthode de calcul :** • Taux d'exception = exceptions actives ÷ nombre total de vulnérabilités non corrigées × 10 • Durée moyenne des exceptions, nombre d'exceptions par motif.
Couverture des analyses avec authentifiants (efficacité de la découverte des actifs)	**Justification :** Cette mesure veille à ce que les actifs connus fassent régulièrement l'objet d'une analyse avec authentifiants. **Méthode de calcul :** actifs analysés régulièrement au moyen d'authentifiants ÷ nombre total d'actifs connus × 100.
Taux de réussite de l'application des correctifs	**Justification :** Cette mesure évalue la fiabilité du processus d'application des correctifs. **Méthode de calcul :** nombre de correctifs appliqués avec succès ÷ nombre de tentatives d'application de correctifs × 100.

	Taux de réouverture	**Justification :** Cette mesure permet de faire le suivi de la fréquence à laquelle les vulnérabilités réapparaissent après avoir été corrigées. Un taux de réouverture élevé indique des problèmes liés à la validation des correctifs, aux retours en arrière ou à la gestion de la configuration. **Méthode de calcul :** (nombre de vulnérabilités réapparaissant pour le même actif dans un délai de N jours ÷ nombre total de vulnérabilités corrigées au cours de la même période) × 100 *(valeurs courantes de N : 30, 60 ou 90 jours).*

Mesures liées à la gestion	**Tendance d’exposition aux risques (cote combinée)**	**Justification :** Cette mesure offre une vue d’ensemble stratégique pour déterminer si les risques organisationnels augmentent ou diminuent. **Méthode de calcul :** fiche d’évaluation pondérée (par exemple, vulnérabilités exploitées connues × 3 + temps moyen de correction × 2 + vulnérabilités critiques non corrigées × 1).
	Services opérationnels à risque élevé	**Justification :** Cette mesure établit des liens entre les vulnérabilités, les résultats opérationnels et les risques d’interruption des services. **Méthode de calcul :** nombre de services présentant des vulnérabilités critiques non résolues.
	Délai relatif à l’acceptation du risque ou à la prise de décision en matière d’atténuation	**Justification :** Cette mesure évalue la réactivité de la structure de gouvernance et la tolérance au risque. **Méthode de calcul :** date de la décision — date de détection (moyenne).

	Nouvelles vulnérabilités et vulnérabilités corrigées	**Justification :** Cette mesure indique si les corrections suivent le rythme des nouvelles vulnérabilités. **Méthode de calcul :** pour chaque mois : • nouvelles vulnérabilités = nombre de vulnérabilités détectées pour la première fois au cours du mois; • vulnérabilités corrigées = nombre de vulnérabilités corrigées au cours du mois; • tendance = (nombre total de vulnérabilités du mois précédent + nouvelles vulnérabilités) - vulnérabilités corrigées.

Toutes les mesures doivent faire l'objet d'une analyse mensuelle ou trimestrielle des tendances pour mettre en évidence la progression, la stagnation ou la régression. Les tableaux de bord, les graphiques et les matrices des risques aident les décideurs à mieux visualiser les tendances.

Dans la mesure du possible, les mesures doivent être réparties selon :

- l'unité opérationnelle;
- le service opérationnel ou l'application;
- le responsable ou l'équipe technique;
- l'emplacement géographique ou la classification (par exemple, systèmes protégés, systèmes classifiés).

Cette répartition permet de cerner les secteurs à risque, de constater les améliorations apportées et de préciser les responsabilités organisationnelles.

Notes de bas de page

1 Secrétariat du Conseil du Trésor du Canada, Directive sur la gestion de la sécurité

2 Centre canadien pour la cybersécurité, Les 10 mesures de sécurité des TI visant à protéger les réseaux Internet et l'information (ITSM.10.089).

3 Centre canadien pour la cybersécurité, Correction des systèmes d'exploitation et des applications – Bulletin de sécurité des TI à l'intention du gouvernement du Canada (ITSM-96).

Date de modification : 2026-04-27

xx
yy