Centre de la sécurité des télécommunications
Communications Security Establishment

CENTRE CANADIEN POUR LA CYBERSÉCURITÉ

Utilisation de la gestion des biens de technologies de l'information (GBTI) pour renforcer la cybersécurité

SÉRIE GESTIONNAIRES

ITSM.10.004

Canada

Avant-propos

La présente publication est un document NON CLASSIFIÉ publié avec l'autorisation du dirigeant principal du Centre canadien pour la cybersécurité (Centre pour la cybersécurité). Pour obtenir de plus amples renseignements, veuillez communiquer par téléphone ou par courriel avec le Centre d'appel du Centre pour la cybersécurité :

contact@cyber.gc.ca
613-949-7048 ou 1-833-CYBER-88

Date d'entrée en vigueur

Le présent document entre en vigueur le 12 avril 2023

Historique des révisions

Version	Modifications	Date
1	Première version.	12 avril 2023

ISBN 978-0-660-48192-0
CAT D97-4/10-004-2023F-PDF

Vue d'ensemble

La présente publication offre aux organisations des avis et des conseils relatifs à la gestion des biens de technologies de l'information (TI) (GBTI). Par ailleurs, elle vous aidera à mieux comprendre la GBTI, en quoi elle consiste, son importance à l'égard de la cybersécurité et les points que votre organisation devrait considérer pour assurer le suivi, la surveillance et le maintien de ses biens de TI. Les organisations de toutes tailles peuvent se baser sur ces conseils pour définir l'ensemble des pratiques, adaptées à leurs exigences opérationnelles, qui leur permettront de suivre et de gérer les biens de TI dans leur environnement.

En mettant en œuvre un processus de GBTI, votre organisation sera en mesure de réduire les coûts de maintenance liés à ses biens de TI, d'utiliser des licences plus efficacement, d'augmenter l'utilisation des biens et de mieux gérer les risques liés à la sécurité. Vous serez en outre mieux préparé pour les vérifications de conformité et vous serez en mesure d'accroître l'efficacité d'autres processus de la bibliothèque d'infrastructure des TI (ITIL pour *Information Technology Infrastructure Library*).

La GBTI est un composant important de tout cadre de gestion des risques liés à la sécurité, notamment l'ITSG-33, La gestion des risques liés à la sécurité des TI : Une méthode axée sur le cycle de vie [1], le NIST Cyber Security Framework [2] et l'ISO/IEC 27001:2013 [3]. L'intégration de la GBTI au cadre de sécurité de votre organisation contribuera à améliorer votre posture de cybersécurité et à offrir une assurance de la sécurité en matière de confidentialité, d'intégrité et de disponibilité pour les biens de l'entreprise.

Les organisations qui n'ont pas les moyens financiers ou ne disposent pas des ressources humaines nécessaires pour mettre en œuvre un cadre de cybersécurité en profondeur sont invitées à appliquer les Contrôles de cybersécurité de base pour les petites et moyennes organisations [4]. Cette publication vous aidera à déterminer les biens précieux de votre organisation en évaluant le niveau de préjudice associé à ceux-ci. Ce faisant, vous serez en mesure de classer adéquatement par catégories vos biens de TI, de choisir les outils de surveillance et de suivi appropriés, ainsi que les contrôles de sécurité nécessaires pour renforcer votre posture de cybersécurité.

Table des matières

Liste des figures

Liste des annexes

1 Introduction

Les activités commerciales de votre organisation ont considérablement changé en ce qui a trait au suivi des biens. Les organisations ont délaissé l'utilisation de feuilles de calcul électroniques en ligne pour faire le suivi des biens. Si vous êtes aux prises avec un trop grand nombre de biens à suivre manuellement, le recours à un outil plus efficace peut s'avérer nécessaire pour gérer votre inventaire. Assurer le suivi de tous les biens est essentiel pour garantir la cybersécurité et la réussite opérationnelle et financière de toute entreprise et organisation.

La GBTI consiste en un processus continu servant à maintenir à jour l'inventaire de tous les biens de TI, qu'ils soient corporels ou incorporels. Il s'agit en fait d'un ensemble de politiques et de processus qui sont utilisés pour aider les organisations à comptabiliser tous les biens, et ce, tout au long de leur cycle de vie. La GBTI joue un rôle important dans la réussite et la croissance d'une organisation. En effet, qu'il s'agisse de gérer les biens de TI en temps réel ou d'acquérir une meilleure visibilité, une gestion efficace des biens de TI permet une détection, une intervention et une résolution rapides en cas d'incident, ce qui contribue à réduire au minimum les pertes de l'organisation.

Selon l' International Association of Information Technology Managers (IAITAM) Global (en anglais seulement) [5], la gestion des biens de TI consiste en un ensemble de pratiques commerciales comprenant les biens de TI dans l'ensemble des unités fonctionnelles de l'organisation. Elle intègre les responsabilités relatives à la gestion des finances, de l'inventaire, des contrats et des risques pour gérer le cycle de vie global de ces biens, notamment la prise de décisions tactiques et stratégiques.

Le recours à un solide processus de GBTI assurera que les biens sont déployés, mis à niveau et éliminés au bon moment et de manière adéquate. Ce processus permet également aux organisations de quantifier les risques et de veiller à ce que tous les biens soient correctement configurés, convenablement protégés et à jour sur le plan des contrôles de sécurité et des correctifs logiciels.

2 Qu'est-ce qu'un bien de TI?

Le réseau de plus en plus complexe d'appareils connectés fait en sorte qu'il est difficile de déterminer ce qui constitue un bien de TI. Considérez un bien de TI comme étant n'importe quel élément faisant partie des systèmes de TI de votre organisation et dont la compromission, la modification ou l'absence pourrait entraîner un préjudice ou avoir de sérieuses répercussions sur vos données et logiciels s'il faisait l'objet d'une fuite ou d'une modification, ou s'il devenait inaccessible. On entend par « biens de TI précieux » les données, les systèmes de TI, les appareils, le matériel ou tous les autres composants importants de l'infrastructure réseau de votre organisation qui contiennent des données sensibles ou qui sont utilisés pour accéder à ces données. Par exemple, un ordinateur de bureau, un ordinateur portable, une tablette ou un téléphone mobile seraient considérés comme un bien, ainsi que les applications et le logiciel exploités sur ces appareils.

La présente publication porte sur trois catégories de biens de TI qui, à notre avis, sont les éléments prioritaires à répertorier et à surveiller. Les trois catégories principales sont les logiciels, le matériel informatique et les données essentielles ou sensibles. Les sous-sections suivantes présentent des observations complémentaires utiles pour votre organisation au moment d'examiner les biens se trouvant dans ces catégories.

2.1 Logiciels

La catégorie des logiciels comprend tous les fichiers et toutes les applications exécutés par une organisation à des fins professionnelles. Seuls des logiciels approuvés et sécurisés devraient être installés sur les appareils de l'organisation. Ces logiciels doivent faire l'objet d'une surveillance active pour s'assurer que les mises à jour et correctifs nécessaires ont été appliqués afin d'éviter que des auteures et auteurs de menace exploitent des vulnérabilités de sécurité. Outre les mises à jour logicielles, les organisations devraient également assurer le suivi ou la surveillance de ce qui suit :

- les applications, les programmes logiciels et les outils de développement;
- les licences des logiciels;
- les abonnements aux logiciels infonuagiques;
- les abonnements aux logiciels-services (SaaS pour *Software as a Service*).

La GBTI pour les logiciels permet aux organisations de surveiller l'état de conformité des contrats de licence, de planifier les licences ultérieures et d'établir le nombre et les types de licences nécessaires pour s'assurer d'obtenir une valeur optimale pour chaque utilisation de licence de logiciel. Il est recommandé que votre organisation ait recours au suivi automatisé des biens pour être en mesure de comptabiliser à la fois les abonnements aux logiciels traditionnels et les abonnements aux logiciels-services.

2.2 Matériel informatique

La catégorie du matériel informatique comprend tous les dispositifs physiques qui composent l'infrastructure de TI d'une organisation. Lors de la gestion de ces dispositifs à chaque étape de leur cycle de vie, les organisations sauront à quel moment elles devront remplacer, mettre à niveau ou faire réparer ces dispositifs. Le matériel informatique se divise en trois catégories :

- Matériel d'infrastructure : tous les principaux composants physiques de l'infrastructure de TI d'une organisation, comme les serveurs physiques, les dispositifs de stockage, les routeurs et les commutateurs.
- Appareils utilisateurs : appareils utilisés au bureau comme les ordinateurs de bureau, les claviers, les moniteurs, les imprimantes et les photocopieurs, et appareils mobiles comme les téléphones intelligents, les tablettes et les ordinateurs portables.
- Dispositifs de l'Internet des objets (IdO) : objets pouvant se connecter à Internet pour recueillir et échanger de l'information avec d'autres dispositifs et systèmes sur Internet. Ces objets « intelligents » sont dotés de capacités supérieures à celles d'ordinateurs, de téléphones intelligents ou de tablettes standards. Ils comprennent notamment les capteurs, les caméras, les microphones, l'équipement de téléconférence, les tableaux blancs interactifs et d'autres appareils à commande vocale.

2.3 Données importantes

La catégorie des données comprend les données utiles et sensibles qui doivent être considérées comme un bien de TI essentiel. Ces données doivent systématiquement être suivies, gérées, maintenues et éliminées en toute sécurité en suivant le cycle de vie de l'information. Ce cycle de vie est semblable à celui suivi pour les composants matériels ou logiciels de votre infrastructure de TI. Il est tout aussi important de gérer et de surveiller les données sensibles que de faire le suivi du matériel ou des logiciels, car les données compromises peuvent avoir des répercussions onéreuses pour votre organisation, à savoir des responsabilités légales coûteuses et des pertes financières considérables. Il est recommandé de mettre en œuvre les mesures suivantes pour vous aider à gérer les biens de données :

- tenir un inventaire des données stockées;
- documenter l'emplacement des données stockées;
- mettre en œuvre des politiques et des contrôles de gestion de l'accès, comme le contrôle d'accès basé sur les rôles (RBAC pour *Role-Based Access Control*), pour s'assurer que l'accès aux données est accordé uniquement aux personnes qui en ont besoin;
- gérer la transmission des données au moyen de méthodes tels le chiffrement par liaison radio, le réseau privé virtuel (RPV) et le chiffrement PGP (*Pretty Good Privacy*);
- gérer le cycle de vie des données à partir du moment où elles ont été générées initialement ou saisies jusqu'à leur éventuel archivage ou suppression à la fin de leur cycle de vie.

3 Pourquoi les organisations ont-elles besoin d'un processus de GBTI?

L'objectif principal de la GBTI est de créer et de maintenir un référentiel de biens qui comporte un inventaire exact, actuel et complet de tous les biens de TI de votre organisation. La surveillance de vos biens de TI vous donne une vue claire de tous les biens, ce qui vous permettra de mieux comprendre ce qui suit :

- les matériels informatiques et les logiciels existants, ainsi que les données qu'ils contiennent;
- l'endroit où résident ces composants de TI dans l'infrastructure;
- l'utilisation qui en est faite et les personnes qui les utilisent;
- leur coût d'achat, de fonctionnement, de maintenance et d'élimination;
- leur connexion à d'autres composants de TI;
- la phase actuelle de leur cycle de vie;
- leur incidence sur les opérations de TI et commerciales.

Un programme de GBTI, appuyé par des processus et des systèmes appropriés, peut offrir à votre organisation une meilleure évolutivité, des économies, une utilisation optimisée des biens et de meilleurs processus de prises de décisions d'affaires en permettant à votre organisation de réaliser ce qui suit :

- assurer le suivi et la maintenance automatiques des biens de TI à mesure que des changements sont apportés dans l'environnement de TI
- relever les biens de TI manquants;
- documenter tout problème de sécurité lié au matériel pouvant accroître le risque pour la sécurité de l'organisation;
- quantifier le coût des biens de TI sous-utilisés;
- prévoir les besoins à venir en matière de capacité de TI;
- rester conforme, se préparer aux vérifications et atténuer les risques juridiques et de sécurité.

4 Avantages de la GBTI sur le plan de la cybersécurité

Un programme de GBTI efficace fait partie intégrante de la stratégie de cybersécurité de votre organisation. Pour être en mesure de protéger vos ressources de TI, vous devez assurer le suivi et la gestion de tous les composants de votre infrastructure de TI. Il vous sera ainsi possible de relever le matériel et les logiciels désuets et de réduire au minimum leur vulnérabilité aux attaques. La GBTI contribue à préserver la confidentialité, l'intégrité et la disponibilité de l'information pour s'assurer que celle-ci n'est pas compromise lorsque surviennent des événements critiques.

Un programme de GBTI solide aidera votre organisation à assurer le suivi et la maintenance des biens à mesure que des changements sont apportés dans votre environnement de TI. En ayant des renseignements à jour et précis sur tous les biens, votre organisation sera en mesure de prendre des décisions éclairées sur les ressources disponibles et leur utilisation. Elle pourra de plus accroître la productivité et l'utilisation globales de ces biens.

Voici quelques raisons pour lesquelles vous devriez ajouter la GBTI à votre **stratégie de cybersécurité :**

1. **Elle atténue les risques :** Une fois le processus de GBTI en place, il est possible d'atténuer les menaces et les risques pour la sécurité qui proviennent de biens de TI dangereux, désuets, perdus ou mal configurés.
2. **Elle améliore la résilience en cybersécurité et assure une intervention plus rapide en cas d'incident :** La GBTI permet aux organisations de se concentrer sur leurs biens les plus précieux et essentiels en mettant en œuvre les bons contrôles de sécurité. Elle procure une visibilité pour qu'il soit facile de cerner le bien touché par un incident, et elle peut faciliter l'analyse des causes fondamentales. La GBTI peut également contribuer à déclencher des interventions plus rapides en cas d'incident et à appliquer des mesures correctives en réponse à des alertes de sécurité en révélant l'emplacement, la configuration et le propriétaire de l'appareil touché.
3. **Elle s'assure que les logiciels sont à jour et corrigés :** Un processus de GBTI permet la gestion des logiciels, ce qui peut aider à relever les logiciels désuets ou non corrigés. D'anciennes versions de logiciels ou des logiciels non corrigés peuvent constituer un risque pour la sécurité de votre organisation.
4. **Elle détermine le rôle de chaque bien logiciel :** Un processus de GBTI vous permettra d'établir tous les logiciels en cours d'utilisation pour veiller à l'obtention des licences adéquates et éviter des achats inutiles. Connaître la fonctionnalité opérationnelle de chaque logiciel permettra de réaliser une configuration adéquate et d'atténuer les risques pour la sécurité.
5. **Elle assure le contrôle des biens matériels :** Lorsque vous utilisez des outils de GBTI, vous pouvez établir les appareils qui sont connectés au réseau et savoir s'ils sont correctement configurés et conformes aux contrôles de sécurité et aux mises à jour actuelles. Les outils peuvent également déterminer les biens matériels désuets et vous aider à prendre les mesures nécessaires pour réduire au minimum les menaces de sécurité découlant du vol ou de la perte de biens.

6. **Elle détermine les contrôles de sécurité pour les biens de TI :** Lors de la mise en œuvre d'un processus de GBTI, vous devrez déterminer les fonctionnalités opérationnelles des biens de TI ainsi que les contrôles de sécurité nécessaires pour les protéger. Lorsqu'un incident se produit, un processus de GBTI vous aide à obtenir une carte claire des réseaux de TI. Vous pourrez alors établir les points de défaillance et les mesures à prendre afin de les corriger et ainsi assurer la continuité des activités.

7. **Elle assure la catégorisation des biens de TI :** Un processus de GBTI exige que les biens soient classés par catégories en fonction de leurs fonctionnalités opérationnelles et de la sensibilité de l'information à gérer. Les biens de TI qui gèrent de l'information sensible doivent être catégorisés comme essentiels et sécurisés à l'aide des bons outils et, en cas de compromission, ils doivent pouvoir faire appel à un processus d'intervention en cas d'incident afin de limiter au maximum toute atteinte à l'organisation.

4.1 Avantages d'un processus de GBTI sur l'ensemble des activités de l'organisation

1. **Améliore la visibilité et le contrôle de l'infrastructure de TI :** Un processus de GBTI permet de recenser les composants de TI connectés au réseau d'une organisation, leur emplacement, leur utilisation, leur état actuel et l'incidence qu'ils ont sur les opérations. Il offre une visibilité des biens de TI qui sont surutilisés, sous-utilisés et désuets. Cette visibilité aide les organisations à améliorer le rendement et l'efficacité de leurs biens ainsi que de leurs coûts indirects.

2. **Aide à déterminer et à suivre les problèmes d'intégrité de la chaîne d'approvisionnement :** La GBTI offre un plus haut niveau de transparence pour la gestion des biens, ce qui assure par conséquent une reddition de comptes. Elle améliore la visibilité de la chaîne d'approvisionnement de l'organisation et appuie le suivi et l'évaluation des problèmes relatifs à l'intégrité de la chaîne d'approvisionnement (ICA). En cas d'incident, il importe de connaître l'origine de vos biens (fabricant, fournisseur ou développeur) et de savoir quand a été effectué la maintenance et par qui. Ces renseignements peuvent aider à déterminer les répercussions que peut avoir le problème d'ICA, ce qui est particulièrement important lorsque le problème est constaté plusieurs années après le déploiement initial du bien. De façon similaire, et avec les dossiers de maintenance à l'appui, les correctifs de micrologiciels appliqués au matériel et les versions de micrologiciels doivent également être suivis de près.

3. **Assure la conformité et une préparation optimisée pour les vérifications :** La tenue d'un inventaire de tous les biens aidera sans doute les organisations à maintenir leur conformité et à se préparer aux vérifications afin de réduire les risques juridiques. Les outils de GBTI peuvent faciliter le contrôle des obligations juridiques, contractuelles et réglementaires tout en réduisant les coûts et les délais de présentation des rapports de vérification.

4. **Appuie d'autres pratiques ITIL :** Le processus améliore l'efficacité d'autres pratiques ITIL en fournissant de l'information sur les biens touchés par un incident, un problème ou un changement au sein de l'infrastructure. Lorsqu'elles connaissent les biens qui ont été touchés, les organisations peuvent alors déterminer la gravité de l'incident et son incidence en effectuant une analyse des causes fondamentales.

5. **Réduit au minimum le coût global :** Le processus permet de réduire les coûts en veillant à ce que les inspections et la maintenance courantes soient réalisées, optimisant ainsi l'utilisation des biens existants. Il

permet également d'empêcher les achats inutiles de biens de TI en quantifiant le coût des biens matériels et logiciels non utilisés. En faisant le suivi des biens tout au long de leur cycle de vie, les organisations s'assurent d'optimiser les dépenses de TI en prenant des décisions sur les besoins opérationnels et en matière de capacités de TI futures. La GBTI peut également contribuer à améliorer la planification budgétaire et d'autres processus décisionnels stratégiques.

5 Cycle de vie des biens de TI

Tous les biens de TI ont une durée d'utilisation définie, et pour maximiser cette utilisation, votre organisation doit gérer et surveiller de manière proactive les biens de TI à chaque étape de leur cycle de vie. C'est ce qu'il convient d'appeler la gestion du cycle de vie des biens de TI (GCVBTI), un processus essentiel de la GBTI. Ce processus aide les organisations à améliorer la productivité en leur permettant de prendre des décisions informées sur les besoins et les services en matière de technologie de l'information. La GCVBTI contribue à optimiser l'efficacité des biens et à réduire les dépenses inutiles ainsi que les coûts de maintenance.

Il est possible que les organisations définissent chaque étape du cycle de vie des biens de différentes façons, mais les phases qui sont généralement reconnues sont illustrées ci-dessous dans la figure 1.

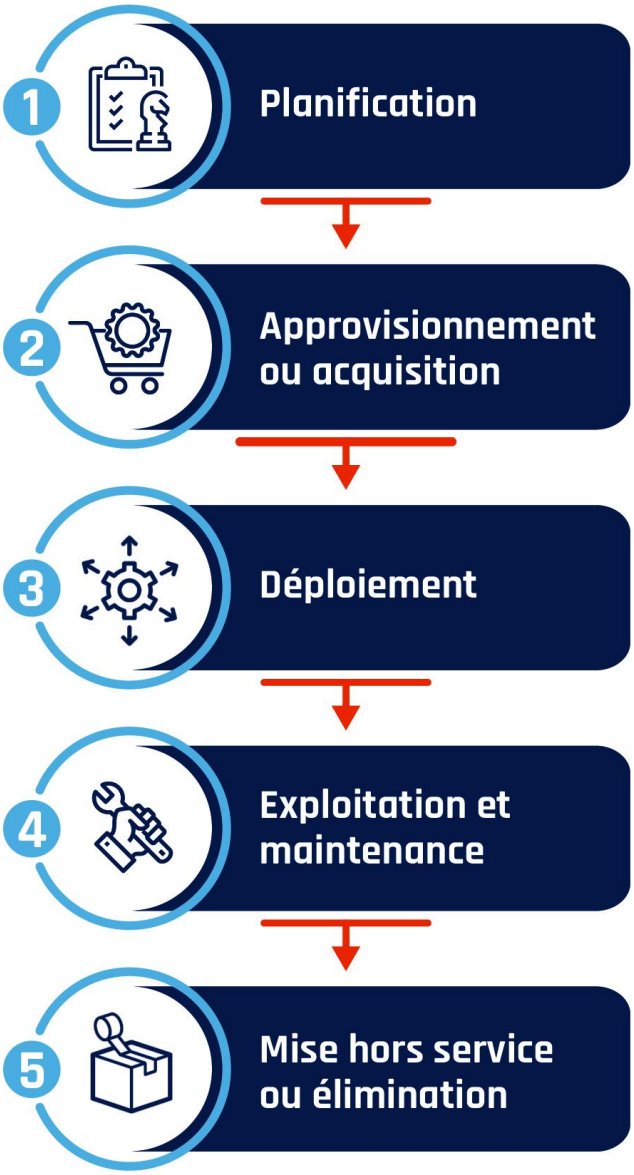

Figure 1 : Cycle de vie des biens

Description de la figure 1 : Les phases les plus courantes du cycle de vie d'un bien sont la planification, l'approvisionnement ou l'acquisition, le déploiement, l'exploitation et la maintenance, et la mise hors service ou l'élimination.

1. **Planification :** La première phase est la planification, et elle devrait en principe avoir lieu avant l'achat du bien. Les organisations doivent déterminer les besoins opérationnels et en matière de sécurité pour ce bien en gardant à l'esprit l'intégrité de la chaîne d'approvisionnement. Elles doivent justifier l'utilisation qui sera faite du bien, son financement et sa contribution aux activités de l'organisation en fonction de l'évaluation des biens existants et de critères préétablis. Un outil de GBTI peut servir à analyser les tendances et les

données, et pourrait aider à déterminer un besoin ultérieur en prédéterminant la valeur que ce bien ajouterait aux opérations.

2. **Approvisionnement ou acquisition :** La deuxième phase est l'approvisionnement ou l'acquisition du bien. Il s'agit de la phase de négociation des coûts, au cours de laquelle les organisations cherchent à déterminer le moyen le plus efficace de répondre à leurs exigences en matière d'objectif, de budget et de délai d'exécution. S'il est établi que le bien est une ressource importante et nécessaire, il est alors acheté, loué, autorisé sous licence ou fabriqué et ensuite installé ou livré à l'endroit déterminé. À ce stade, le suivi du bien peut se faire tout au long de son cycle de vie à l'aide d'un système de gestion des biens.

3. **Déploiement :** La phase de déploiement, aussi appelée phase d'utilisation, est la plus courte du cycle de vie d'un bien. Elle se produit lorsque des inspections préliminaires sont menées pour s'assurer que le bien fonctionne correctement et de manière sûre. Au cours de cette phase, le bien est présenté aux opératrices et opérateurs ainsi qu'aux employées et employés, et il est intégré à l'infrastructure de TI de l'organisation où il aura une interaction avec d'autres biens pour générer une valeur accrue.

4. **Exploitation et maintenance :** La phase d'exploitation et de maintenance est la plus longue et nécessite souvent le plus de ressources et d'attention. Avec le bien installé et intégré à l'infrastructure de TI, celui-ci peut maintenant améliorer les opérations et générer une valeur commerciale. Pour maximiser cette valeur et prolonger la durée de vie du bien, il est essentiel de procéder à une maintenance systématique, à des suivis continus, à des réparations, à des mises à niveau et à des mises à jour courantes. Des ajustements devront être apportés au bien pour respecter les exigences opérationnelles et de sécurité, maximiser les investissements et procurer une valeur permanente.

5. **Mise hors service ou élimination :** Lorsqu'un bien n'est plus utile ou rentable pour une organisation, et qu'il ne fonctionne plus efficacement, ou que les coûts d'exploitation et de maintenance deviennent trop élevés, il passe à la dernière phase, soit la mise hors service ou l'élimination. À cette étape, le bien doit être désactivé, vendu ou éliminé d'une manière sûre et respectueuse de l'environnement. Toutefois, si le bien est toujours requis sur le plan opérationnel, un bien de remplacement est à prévoir et le cycle de vie des biens recommence.

À la fin de la vie utile du bien, les organisations doivent suivre la réglementation environnementale en vigueur et procéder à une élimination sûre et durable du bien. Les biens qui comportent de l'information sensible devront être nettoyés avant leur élimination en supprimant toutes les données et dans certains cas en détruisant les supports qui contiennent les données, tel qu'il est décrit dans la publication Nettoyage des supports de TI (ITSP.40.006) [6] et dans la Directive sur la gestion du matériel du gouvernement du Canada (GC) [7].

6 Pratiques exemplaires en matière de GBTI

La GBTI se veut un processus continu plutôt qu'un projet ponctuel. Il faut l'intégrer aux pratiques opérationnelles de l'organisation et en assurer le maintien régulièrement. Votre organisation peut commencer le processus de mise en œuvre et de maintien de la GBTI en réalisant les tâches suivantes :

1. Déterminer les ressources nécessaires pour élaborer le processus de GBTI;
2. Préciser les capacités nécessaires pour créer un processus de GBTI qui respectera les besoins opérationnels, les objectifs et le budget;
3. Former une équipe composée de membres exerçant des responsabilités précises pour gérer le processus de GBTI;
4. Déterminer qui est chargé des différentes fonctions liées à la GBTI :
    - établissement et catégorisation des biens;
    - suivi des licences de logiciel;
    - établissement des risques et intervention;
    - surveillance et production de rapports.

Voici quelques pratiques exemplaires que devrait suivre votre organisation dans le cadre du processus d'élaboration de la GBTI. Certaines de ces activités peuvent être mises en correspondance avec les contrôles de sécurité trouvés dans l'ITSG-33, La gestion des risques liés à la sécurité des TI : Une méthode axée sur le cycle de vie [1]. Les contrôles de sécurité qui sont pertinents à l'activité en question sont indiqués entre parenthèses. Pour en savoir plus sur les contrôles énumérés ci-dessous, consultez l'annexe A du présent document.

1. Créer un dossier d'inventaire complet

   (CM-8 Inventaire des composants de système d'information)

   Après avoir élaboré votre plan de GBTI, la prochaine étape consiste à créer un dossier d'inventaire précis qui comprend les biens de TI matériels et logiciels, les données et les licences. Un dossier complet de tous les biens permet à votre organisation de connaître les biens qu'elle détient, leur emplacement et les personnes qui en sont responsables. Il permet également d'éviter des achats en double et de cerner de possibles responsabilités légales et visant la sécurité.

2. **Mettre régulièrement à jour l'inventaire des biens**

   (CM-8 Inventaire des composants de système d'information avec amélioration de contrôle 1)

   Cette activité est essentielle afin de s'assurer que tous les biens ont été correctement comptabilisés.
   Elle peut entre autres déterminer le moment où les biens se déprécient et aider à établir un budget pour les

travaux de maintenance et de remplacement à venir. Chaque bien nouvellement acquis et intégré à l'infrastructure de l'organisation doit être immédiatement ajouté à l'inventaire.

3. **Classer les biens par catégories**

   (RA-2 Catégorisation de sécurité)

   Il est important de catégoriser les biens et de déterminer ceux qui sont les plus essentiels afin de permettre à votre organisation d'affecter des ressources afin de les gérer et de les sécuriser adéquatement.

4. **Adopter une approche de gestion du cycle de vie**

   (PE-20 Surveillance et suivi des biens)

   L'un des aspects les plus importants de la gestion des biens de TI consiste à bien comprendre le cycle de vie des biens. La durée de vie de chaque bien varie. Il est donc important de faire le suivi de chaque bien tout au long de son cycle de vie pour aider à déterminer à quel moment le bien devient désuet et doit être remplacé ou mis à niveau.

   Une administratrice ou un administrateur de TI désigné doit se servir d'un processus de gestion des inventaires qui lui permet de surveiller et de documenter l'état du cycle de vie de chaque bien de TI. Ce processus indique si un bien est en cours d'utilisation, stocké, emprunté, disponible ou hors service. Il permet de mieux surveiller et d'améliorer la cybersécurité d'une organisation, car les biens désuets entraînent des vulnérabilités que les auteures et auteurs de menace peuvent exploiter.

5. **Automatiser la GBTI**

   (CM-8 Inventaire des composants de système d'information avec améliorations de contrôle 2 et 3 et MA-6 Maintenance opportune avec amélioration de contrôle 3)

   L'automatisation peut contribuer à améliorer les pratiques de GBTI de votre organisation, à accroître la productivité et à réduire le risque d'erreur humaine. L'organisation devrait utiliser des outils pour remplacer le personnel technique qui accomplit des tâches répétitives ou redondantes. Par exemple, il existe des programmes logiciels qui peuvent automatiser le processus de suivi des biens. Ces programmes veillent à ce que les biens fassent l'objet d'un suivi adéquat et continu pour que rien ne soit oublié.

   L'automatisation peut également être utile pour les analyses périodiques planifiées et les alertes automatiques. Ces vérifications automatisées aident à cerner les biens qui ont besoin de maintenance ou de mise à niveau, et elles envoient des alertes au personnel technique pour qu'il corrige les problèmes.

6. **Assurer le suivi des licences de logiciels**

   (CM-8 Inventaire des composants de système d'information)

Un aspect important de la GBTI est de bien gérer et documenter les licences de logiciels. Une licence de logiciel (aussi appelée certificat) constitue essentiellement un contrat entre l'acheteuse ou acheteur et la vendeuse ou le vendeur. Ce contrat définit les droits d'installation et les garanties, et il stipule les responsabilités. Les organisations doivent connaître les logiciels qu'elles sont autorisées à déployer et leur date d'expiration, et elles doivent également savoir si ces logiciels ont besoin d'être renouvelés, mis à jour ou annulés. Ces renseignements sont excessivement importants et permettront aux organisations d'être bien préparées aux vérifications de logiciels.

7. **Tenir des dossiers de tous les travaux de maintenance effectués sur le bien**

   (MA-2 Maintenance contrôlée avec amélioration de contrôle 2)

   Faire le suivi de la maintenance effectuée sur un bien tout au long de son cycle de vie s'avère utile pour déterminer les problèmes d'intégrité de la chaîne d'approvisionnement imputables aux fournisseurs de services de maintenance.

8. **Intégrer la GBTI à d'autres activités de TI au sein de l'organisation**

   La gestion des biens de TI n'est qu'une partie d'une stratégie de cybersécurité plus vaste et doit être intégrée aux activités de TI de l'organisation, comme la gestion des services de TI (GSTI) et la gestion des risques liés aux TI. Le cadre ITIL, par exemple, intègre des processus de GBTI pour atteindre ces objectifs.

9. **Vérifier et améliorer continuellement les politiques et les processus de GBTI**

   (AU-6 Examen, analyse et rapports de vérification et AU-7 Réduction des vérifications et génération de rapports)

   La gestion de biens de TI n'a rien d'un projet ponctuel. Elle est plutôt un processus continu qui comprend des pratiques de vérification et d'amélioration au besoin. Les vérifications annuelles des biens de TI aident à suivre ce qui doit être mis à jour ou remplacé. Cette information permet à votre organisation de prendre des décisions éclairées relatives à son budget, à ses achats à venir et à ses objectifs; elle aide également à établir les points qui nécessitent une amélioration.

   Votre organisation peut s'assurer que ses systèmes de TI demeurent à jour en évaluant chaque année les biens qu'elle possède en faisant le suivi des indicateurs de rendement clés ainsi que d'autres données pertinentes. Il est également essentiel de recueillir les commentaires. Cette pratique facilite une amélioration continue et vous aide à planifier les changements à apporter à votre processus de GBTI, le cas échéant.

10. **Gérer adéquatement les biens anciens, expirés ou désuets**

    (MP-6 Nettoyage des supports : contrôles A et B)

Lorsqu'un bien ne fonctionne plus efficacement ou n'est plus rentable pour une organisation, et que les coûts d'exploitation et de maintenance deviennent trop élevés, il est recommandé de mettre à niveau et d'éliminer ce bien. Lors de l'élimination de biens de TI, les organisations doivent respecter des normes réglementaires. Le non-respect de ces normes peut entraîner des sanctions financières, des répercussions juridiques et des dommages à la réputation d'une organisation. Toutes les données se trouvant sur un support de stockage matériel doivent être effacées, pour tous les biens qui, à un moment ou à un autre dans leur cycle de vie, ont contenu de l'information sensible. Cette suppression doit se faire avant l'élimination des biens. Pour les ministères et organismes du gouvernement fédéral, il peut s'avérer nécessaire de nettoyer et de détruire le support, tel qu'il est décrit dans la publication Nettoyage des supports de TI (ITSP.40.006) [6].

Les organisations ne sont pas toujours en mesure de mettre à jour leurs biens. Par conséquent, certaines vont choisir de continuer à les utiliser même si ces biens deviennent désuets. Les biens désuets ne reçoivent plus de mises à jour de sécurité ou les plus récentes mesures d'atténuation, ce qui augmente l'incidence des vulnérabilités et le taux d'exploitation. Si une organisation décide malgré tout de continuer à utiliser des biens désuets, nous lui recommandons de consulter la publication *Device Security Guidance du National Cyber Security Centre (NCSC)* [8] et la publication Produits obsolètes (ITSAP.00.095) [9]. Cette publication offre des conseils pour réduire les risques liés à l'utilisation d'appareils désuets comme des téléphones intelligents, des tablettes, des ordinateurs portables, des ordinateurs de bureau, des appliances ou des applications logicielles.

7 Outils pour appuyer les processus de GBTI

Un outil de GBTI est un logiciel servant à gérer les biens de TI tout au long de leur cycle de vie, c'est-à-dire de l'achat à l'élimination. Il s'agit d'un système centralisé qui permet aux organisations de surveiller, de suivre et de catégoriser automatiquement leurs biens de TI en temps réel. Un logiciel de gestion des biens regroupe toutes les tâches essentielles associées au suivi des biens dans une seule plateforme accessible par Internet et par des applications mobiles. Les outils de GBTI peuvent stocker les données suivantes :

- de l'information sur l'inventaire, comme l'emplacement, le propriétaire, l'état et le statut du cycle de vie d'un bien;
- de l'information contractuelle, comme les licences, la garantie des biens, les conventions de soutien et d'autres conditions stipulées dans les contrats;
- de l'information financière, ce qui comprend les prix d'achat, les coûts liés à la maintenance, aux réparations et aux mises à niveau, et l'information sur les fournisseurs.

Lorsque ces données sont regroupées dans un seul endroit, les coûts administratifs sont moindres, l'efficacité du bien est optimisée et l'organisation a une meilleure vue d'ensemble de l'utilisation des biens, des coûts et de la maintenance.

On compte de nombreuses normes et certifications pour la gestion des biens, notamment ISO 55001 [10]. Bien que les organisations ne soient pas tenues de suivre une norme, l'établissement d'une norme peut aider à gérer le cycle de vie des biens de manière plus efficace et à améliorer le rendement des biens de l'organisation.

La norme ISO 55001 est un cadre qui peut aider votre organisation à accroître le contrôle des activités quotidiennes, à assurer un meilleur rendement du capital investi pour les biens, à atténuer les risques et à réduire le coût global. Cette norme peut être appliquée à toutes sortes d'organisations ayant différents types de biens. L'ISO 55001 offre les outils nécessaires pour optimiser la valeur des biens tout en veillant à ce que ces biens respectent les exigences requises en matière de sécurité et de rendement.

Le National Institute of Standards and Technology (NIST) a publié un guide de cybersécurité pour la GBTI. La publication, qui a été écrite de concert avec le National Cyber Security Centre of Excellence (NCCoE), donne un aperçu des fonctions et de la configuration d'un système de gestion des biens. Ce document se veut un guide pour aider les organisations à mettre en œuvre une solution de GBTI. Il s'agit d'une solution de démonstration de concept qui présente les technologies disponibles sur le marché pouvant être mises en œuvre pour faire le suivi de l'emplacement et de la configuration des logiciels et des dispositifs en réseau dans l'ensemble de l'entreprise. Pour obtenir de plus amples renseignements sur cette publication, consultez le document NIST special publication1800-5: IT Asset Management [11].

7.1 Avantages que présente l'utilisation d'outils de GBTI

En plus de ce qui a été mentionné précédemment, les outils de GBTI peuvent offrir les avantages suivants :

1. **Suivi en temps réel des activités et de l'état des biens :**

   Les outils de GBTI peuvent automatiquement faire le suivi et l'enregistrement de différentes activités liées aux biens, telles que les heures d'utilisation, l'emplacement, les modifications et les changements apportés aux biens. Ces actions sont continuellement surveillées et mises à jour dans une base de données en temps réel. L'utilisation d'outils automatisés comme des logiciels et des dispositifs de suivi est une façon plus efficace et accessible de gérer et d'assurer une intervention rapide en cas de problèmes ou de mauvaises utilisations des biens. La majorité des logiciels de suivi des biens offre des fonctionnalités complètes de génération de rapports sur demande.

2. **Élimination de l'erreur humaine et augmentation de la précision :**

   Grâce aux outils automatisés de gestion des biens, les organisations peuvent recueillir et stocker une analytique impartiale, précise et organisée à l'abri de l'erreur humaine. Une erreur humaine peut souvent passer inaperçue durant une longue période, et tenter d'en trouver la source peut être pratiquement impossible. L'automatisation permet d'obtenir un inventaire plus efficace, ainsi qu'un meilleur contrôle et une plus grande précision en ce qui concerne les biens d'une organisation, et ce, tout au long de leur cycle de vie.

3. **Calendrier de maintenance efficace et détection précoce des problèmes :**

   Les outils automatisés de gestion des biens proposent une maintenance préventive. Ils permettent de surveiller l'information sur l'état, l'installation et la garantie d'un bien, ainsi que l'historique de la maintenance (qui l'a effectuée, où et quand). Connaître l'historique de la maintenance contribue également à accroître la responsabilisation. Les outils de gestion des biens peuvent être configurés de façon à envoyer automatiquement des notifications lorsqu'une activité de maintenance est requise. La maintenance peut contribuer à augmenter la durée de vie d'un bien et à cerner les problèmes et les sources d'inefficacité suffisamment tôt pour éviter des coûts élevés de maintenance.

4. **Économie de temps et d'argent :**

   Quelle que soit la taille de l'organisation, effectuer un inventaire manuel des biens peut se révéler une tâche fastidieuse et pourrait nécessiter des efforts de la part de plusieurs membres du personnel. Un système automatisé de suivi des biens peut accroître l'efficacité, de même que permettre des économies de temps et d'argent. L'automatisation du suivi des biens assure que l'information fournie dans la base de données de

gestion des biens est fiable et à jour, et cela peut contribuer à économiser de l'argent en évitant de faire des achats inutiles ou répétitifs.

5. **Amélioration et facilitation des vérifications :**

   Un logiciel automatisé de suivi des biens offre de l'information détaillée sur les biens de l'organisation. Il crée un registre des renseignements requis aux fins de vérification, notamment l'emplacement, l'état, l'information sur la maintenance et le propriétaire des biens. Un tel logiciel facilite et automatise la génération de rapports de vérification précis et permet à l'organisation de rester conforme et de toujours respecter les normes juridiques.

Toutefois, il est important de noter que malgré tous les avantages, la découverte automatique de biens peut soulever des préoccupations, car certains biens peuvent réagir moins bien à une analyse effectuée par ces outils. Les organisations doivent tenir compte de ce point, surtout pour les systèmes de contrôle industriels (SCI) et les infrastructures essentielles pour lesquels la fiabilité et la disponibilité sont des préoccupations de premier plan. Elles devront appliquer différentes stratégies ou méthodologies d'inventaire à ces systèmes. La section 7.3 du présent document offre de plus amples détails à ce sujet.

7.2 Critères à considérer au moment de choisir un outil de GBTI

L'outil de GBTI devrait être doté des capacités et des fonctionnalités nécessaires pour prendre en charge les processus liés aux biens de TI de votre organisation Lors de l'examen des outils de GBTI, assurez-vous de les évaluer en fonction des critères et des fonctionnalités suivants :

1. **Facilité d'utilisation :** La convivialité pour les utilisateurs est probablement le critère le plus important dans le choix d'un logiciel de gestion des biens. Le logiciel doit permettre une navigation et une personnalisation faciles en fonction des exigences et des besoins particuliers de l'organisation. L'outil doit avoir une interface intuitive que les utilisateurs peuvent facilement explorer et apprendre à utiliser.
2. **Découverte automatique de biens :** Tous les biens qui sont connectés à votre infrastructure de TI doivent pouvoir être automatiquement découverts et ajoutés à l'inventaire des biens de TI. Une fois installée, une application de découverte de biens de TI communique avec les dispositifs du réseau pour recueillir de l'information liée au matériel et au logiciel. Cette application peut être configurée de manière à signaler et à retirer régulièrement les biens logiciels redondants affectés à d'anciens employés qui avaient un accès privilégié à votre réseau et à des composants matériels, logiciels et micrologiciels non autorisés au sein de l'infrastructure de TI.
3. **Suivi par métrologie matérielle et logicielle :** Ce suivi comprend le taux d'utilisation, les coûts de surveillance, la garantie, le statut des contrats et des licences, la gestion de la conformité, ainsi que la génération de rapports, d'aperçus et d'alertes.
4. **Intégration et compatibilité :** Il faut s'assurer que le logiciel de GBTI se synchronise bien avec les logiciels en cours d'utilisation et s'intègre sans problème à votre infrastructure de TI.

5. **Information en temps réel :** Le logiciel de GBTI doit fournir de l'information immédiate sur les biens de TI, à mesure que de changements sont détectés. Il doit immédiatement transmettre une notification s'il détecte une mesure au-delà des seuils préconfigurés.

6. **Gestion du cycle de vie de bout en bout :** Chaque bien de TI passe par un cycle de vie, lequel commence par la demande d'achat et se termine par son élimination. Le logiciel de GBTI fera le suivi des biens de votre organisation à chaque étape de leur cycle de vie et aidera à gérer chaque bien du début à la fin. Un tel suivi tout au long de la vie utile des biens permet de garantir de tirer le maximum des biens qui se trouvent dans votre environnement de TI.

7. **Soutien après-vente :** Assurez-vous d'avoir accès à du soutien technique de la part du fournisseur de logiciel de GBTI, même après l'achat de son logiciel. Recherchez une entreprise réputée qui offre une équipe de soutien facilement accessible et prête à apporter rapidement l'assistance requise.

8. **Configuration et personnalisation :** Optez pour un outil qui peut être modifié pour appuyer les exigences de votre organisation.

9. **Évolutivité :** Il est important que le logiciel choisi soit évolutif. Informez-vous au sujet de la souplesse offerte par le logiciel et le fournisseur advenant une demande de modification du produit pour qu'ils répondent aux besoins opérationnels actuels et futurs de votre organisation.

7.3 Critères additionnels à considérer pour les systèmes de TO et les SCI

Les systèmes de contrôle industriels (SCI) patrimoniaux sont souvent sensibles à une augmentation de trafic ou à l'interférence découlant des technologies de balayage comme les outils de découverte. L'utilisation de technologies de balayage sur des SCI pose des risques pour votre organisation, car ces technologies peuvent provoquer des interruptions involontaires des processus. La nature décentralisée d'un réseau de SCI, ainsi que la capacité minimale de l'équipement de réseau patrimonial, rendent difficile l'utilisation de technologies de balayage standards.

Au moment de choisir des outils de découverte de biens à intégrer à une infrastructure de SCI et de technologies opérationnelles (TO), les exploitants doivent savoir comment ces outils interagissent avec les dispositifs qui se trouvent dans le réseau de TO et de SCI. Des outils non compatibles pourraient perturber l'infrastructure en provoquant chez certains dispositifs un comportement irrégulier, comme l'interruption ou le redémarrage du dispositif, ou encore une intervention manuelle requise pour annuler un état de fonctionnement. La liste suivante énonce certains des éléments que les exploitants doivent prendre en considération au moment de choisir des technologies pour le suivi des biens des SCI ou des systèmes de TO :

- s'assurer que la technologie prend en charge les systèmes de contrôle industriels (p. ex. elle tient des profils pour les protocoles de communications de données);
- utiliser des technologies conçues pour les réseaux SCI avec compatibilité d'intégration aux protocoles et aux communications des SCI, comme les capacités d'inspection approfondie des paquets;

- utiliser des technologies qui ne recueillent, ne stockent ou ne partagent pas de données sensibles non autorisées;
- s'assurer qu'une ingénieure ou un ingénieur de TO ou de SCI a approuvé l'utilisation de l'outil pour le SCI ou le système de TO précis.

8 Mappage de réseau pour la gestion des biens

Une partie importante d'un processus de GBTI est le mappage de réseau. Le mappage de réseau consiste en un processus continu de découverte de toutes les entités liées à un réseau pour assurer une visibilité granulaire de l'infrastructure de TI de votre organisation.

Les outils de mappage de réseau peuvent créer une carte virtuelle de votre architecture réseau en découvrant automatiquement les composants et la topologie du réseau. Ces outils peuvent générer des aperçus clés du rendement, comme l'état d'un dispositif, les connexions physiques et la métrologie du trafic. Ils permettent également de visualiser automatiquement, en temps réel, les connexions entre le réseau et les dispositifs, et de déterminer comment différents terminaux, serveurs et équipement réseau communiquent ensemble. Les équipes de TI de votre organisation peuvent ainsi mieux détecter les problèmes et diagnostiquer ceux-ci de manière efficace et rapide afin de limiter les interruptions de service. Outre les avantages déjà mentionnés, le mappage de réseau peut aider à :

- trouver et à corriger des points de défaillance dans le réseau;
- réaliser plus rapidement et facilement l'analyse, la surveillance, la découverte et le diagnostic réseau;
- comprendre la relation entre les différents composants du réseau et les appareils connectés;
- établir l'emplacement des appareils problématiques sur le réseau;
- détecter des connexions suspectes dans le réseau;
- recueillir de l'information qui permet l'analyse des causes fondamentales des problèmes du réseau.

9 Logiciel de gestion des biens fondé sur l'infonuagique

La technologie des services infonuagiques a permis aux organisations de réduire leur espace physique et d'économiser sur les infrastructures coûteuses en éliminant le besoin de stocker leurs serveurs et centres de données sur place. De même, la gestion des biens fondée sur l'infonuagique permet à votre organisation de stocker des données en ligne et d'exécuter des applications sans avoir à installer des logiciels. Votre organisation n'a pas à injecter d'importantes sommes dans des logiciels pour gérer et faire le suivi des biens, car les fournisseurs de services infonuagiques (FSI) offrent souvent de tels services dans le cadre de leur accord sur les niveaux de service (ANS). Les FSI peuvent également fournir un service personnalisable de suivi et de production de rapports pour les biens de votre organisation.

Si votre organisation collabore avec un FSI, vous devez savoir que vous lui donnez alors un contrôle direct de nombreux aspects sur le plan de la sécurité et de la vie privée. Vous devriez discuter avec des FSI pour établir une relation de confiance et veiller à ce que les paramètres de sécurité et les responsabilités soient clairement stipulés dans votre ANS. Malgré le modèle de déploiement infonuagique, votre organisation demeure responsable de la protection de la confidentialité, de l'intégrité et de la disponibilité des services de TI et des renseignements hébergés par le FSI. Les organisations doivent déterminer toutes les exigences opérationnelles et de sécurité applicables à la GBTI et s'assurer que les risques liés à la sécurité sont gérés adéquatement, que les facteurs liés à la sécurité propre à l'infonuagique sont pris en compte et que les contrôles de sécurité des services dans le nuage sont correctement évalués par le FSI. Ce FSI doit être doté d'une politique détaillée en matière de protection et de confidentialité des données. Il doit être conforme aux lois et aux réglementations de plusieurs pays, comme la *Loi sur la protection des renseignements personnels* et la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE) [12] qui régissent la collecte, l'utilisation et la divulgation de renseignements personnels.

Les ministères et organismes du gouvernement du Canada (GC) qui désirent obtenir de plus amples renseignements sur les facteurs à considérer avant de faire appel à un service infonuagique public sont invités à consulter les publications Processus d'évaluation de la sécurité des technologies de l'information s'appliquant aux fournisseurs de services infonuagiques (ITSM.50.100) [13] et Gérer les risques liés aux données du gouvernement du Canada dans le contexte des services infonuagiques (ITSM.50.109) [14].

9.1 Avantages d'une gestion des biens fondée sur l'infonuagique

Un système logiciel de gestion des biens fondé sur l'infonuagique peut offrir à votre organisation un suivi précis, des opérations efficaces, une responsabilité financière et une production de rapports facile. De plus, une approche fondée sur l'infonuagique pour la gestion des biens peut offrir à l'organisation plusieurs autres avantages :

- **Protection de données :** Toutes les données stockées dans le nuage sont chiffrées et un système de gestion infonuagique assure la sécurité des données avec l'aide d'une équipe de sécurité spécialisée qui travaille continuellement dans le but d'éliminer les vulnérabilités.

- **Souplesse :** Certains logiciels de gestion des biens offrent des fonctionnalités favorisant la souplesse et la personnalisation. Les systèmes fondés sur l'infonuagique offrent une souplesse tout en permettant à votre organisation de personnaliser le service de suivi des biens pour répondre à ses besoins opérationnels particuliers.
- **Évolutivité :** Au fur et à mesure que votre organisation prend de l'expansion, il pourrait arriver qu'un logiciel de GBTI ne soit pas en mesure de satisfaire et de suivre l'évolution de vos besoins. Les logiciels fondés sur l'infonuagique sont évolutifs et ils peuvent s'adapter pour répondre aux besoins grandissants des organisations.
- **Intégration :** Certains produits logiciels fondés sur l'infonuagique peuvent facilement être intégrés à l'infrastructure existante de votre organisation pour procurer une visibilité complète et assurer le bon fonctionnement continu des activités.
- **Rentabilité :** L'organisation peut réduire le coût des systèmes de stockage de données et de l'espace physique pour stocker les serveurs.
- **Visibilité accrue :** L'approche infonuagique permet d'accroître la visibilité de l'inventaire des biens et de donner des renseignements plus détaillés pour aider votre organisation à gérer ses biens de la façon la plus rentable possible.
- **Automatisation :** Des outils automatisés sont offerts pour gérer la découverte de biens, et cette automatisation fournit de l'information sur l'inventaire à jour et en temps réel. L'automatisation fait gagner du temps à votre organisation et élimine les risques d'erreurs humaines associées à la gestion des biens dans le nuage. L'automatisation peut également corriger des vulnérabilités lors de leur détection, sans intervention humaine.
- **Conformité :** Il faut procéder à un examen périodique du système de suivi des biens pour s'assurer que toutes les ressources infonuagiques sont suffisamment sécurisées et conformes.

10 Résumé

Cette publication explique comment le processus de GBTI peut aider les organisations de toutes tailles à améliorer et à renforcer leur posture de cybersécurité et à accroître leur résilience face aux cybermenaces. La GBTI se veut un processus continu plutôt qu'un projet ponctuel, et demande d'être évaluée et modifiée régulièrement pour répondre à vos besoins opérationnels en constante évolution. La gestion des biens de TI n'est qu'une composante d'une stratégie de cybersécurité plus vaste, et elle doit être intégrée aux processus ITIL de l'organisation et à son cadre de gestion des risques.

Le présent document énonce les pratiques exemplaires que toutes les organisations devraient mettre en œuvre au moment d'élaborer leur processus de GBTI. Nous recommandons également, dans la mesure du possible, d'automatiser le processus de GBTI. L'automatisation peut contribuer à améliorer l'efficacité de la GBTI, à accroître la productivité et à réduire les risques de sécurité. La gestion des biens fondée sur l'infonuagique est également une option qui s'offre aux organisations qui ne possèdent pas l'espace physique ou les ressources nécessaires pour conserver ou exploiter leurs propres serveurs et centres de données.

En créant un inventaire précis de tous les biens, votre organisation bénéficie d'une meilleure vue d'ensemble de tous les aspects de la cybersécurité et de la conformité. Un processus de GBTI peut vous aider à quantifier les risques et à déterminer ce qui doit être protégé. Il permet d'intervenir rapidement et de façon réfléchie en cas de cyberincident, et ce, en réduisant au minimum les répercussions.

11 Contenu complémentaire

11.1 Liste des acronymes, des abréviations et des sigles

Acronyme, abréviation ou sigle	Définition
FSI	Fournisseur de services infonuagiques
GC	Gouvernement du Canada
IAITAM	*International Association of IT Asset Managers*
SCI	Système de contrôle industriel
IdO	Internet des objets
ISO	Organisation internationale de normalisation (*International Organization for Standardization*)
TI	Technologies de l'information
GCVBTI	Gestion du cycle de vie des biens de TI
ITIL	*Information technology infrastructure library*
GSTI	Gestion des services informatiques (*IT service management*)
NCCoE	*National Cyber Security Centre of Excellence*
NIST	*National Institute of Standards and Technology*
TO	Technologies opérationnelles
PGP	*Pretty Good Privacy*
RBAC	Contrôle d'accès basé sur les rôles (*Role-Based Access Control*)
ANS	Accord sur les niveaux de service
RPV	Réseau privé virtuel

11.2 Glossaire

Terme	Définition
Disponibilité	Caractéristique de l'information ou des systèmes qui sont accessibles aux personnes autorisées au moment où celles-ci en ont besoin. La disponibilité est un attribut des biens d'information, des logiciels et du matériel informatique (l'infrastructure et ses composantes). Il est également entendu que la disponibilité comprend la protection des biens contre les accès non autorisés et les compromissions.
Compromission	Divulgation intentionnelle ou non intentionnelle d'information mettant en péril sa confidentialité, son intégrité ou sa disponibilité.
Confidentialité	Caractéristique de l'information sensible protégée contre tout accès non autorisé.
Infonuagique	Recours à des serveurs distants hébergés dans l'Internet. L'infonuagique permet à des utilisateurs d'accéder à un ensemble de ressources informatiques (comme des réseaux, des serveurs, des applications ou des services) sur demande et de n'importe où. Les utilisateurs accèdent à toutes ces ressources par l'intermédiaire d'un réseau informatique plutôt que d'avoir à les stocker sur leur propre ordinateur.
Infrastructures essentielles	Ensemble des processus, des systèmes, des installations, des technologies, des réseaux, des biens et des services essentiels à la santé, à la sécurité ou au bien-être économique des Canadiennes et Canadiens ainsi qu'au fonctionnement efficace du gouvernement. Il peut s'agir d'infrastructures autonomes ou caractérisées par des interdépendances au sein d'une province ou d'un territoire, entre eux ou au-delà des frontières du pays. La perturbation des infrastructures essentielles pourrait se

Terme	Définition
	traduire en pertes de vie et en effets économiques néfastes, et pourrait considérablement ébranler la confiance du grand public.
Cyberattaque	Recours à des techniques électroniques visant à perturber, à manipuler, à détruire ou à infiltrer un système informatique, un réseau ou un dispositif.
Cybersécurité	Protection de l'information numérique et de l'intégrité de l'infrastructure qui héberge et transmet cette information. Concrètement, la cybersécurité comprend l'ensemble des technologies, des processus, des pratiques et des mesures d'intervention et d'atténuation conçu pour protéger les réseaux, les ordinateurs, les programmes et les données contre les attaques, les dommages ou les accès non autorisés pour ainsi assurer la confidentialité, l'intégrité et la disponibilité.
Chiffrement	Procédure par laquelle une information est convertie d'une forme à une autre afin d'en dissimuler le contenu et d'en interdire l'accès aux entités non autorisées.
Intégrité	Aptitude à protéger l'information contre les modifications ou les suppressions non intentionnelles ou inopportunes. L'intégrité permet de savoir si l'information est conforme à ce qu'elle est censée être. Elle s'applique également aux processus opérationnels, à la logique des applications logicielles, au matériel et au personnel.
Internet des objets	Réseau de dispositifs Web courants capables de se connecter les uns aux autres et d'échanger de l'information.
Bien de TI	Composants d'un système d'information, ce qui comprend les applications opérationnelles, les données, le matériel et les logiciels.
Contrôle de sécurité	Exigence technique, opérationnelle ou gestionnelle de haut niveau relative à la sécurité, qu'il convient d'appliquer à un système d'information afin de protéger la confidentialité, l'intégrité et la disponibilité des actifs TI connexes. Ces contrôles peuvent être appliqués au moyen de diverses solutions de sécurité, notamment des produits, des politiques, des pratiques et des procédures de sécurité.
Information sensible	Information qui doit être protégée contre toute divulgation non autorisée.
Menace	Événement ou acte délibéré, accidentel ou naturel pouvant éventuellement porter préjudice à l'information et aux actifs TI.
Vulnérabilité	Défectuosité ou lacune inhérente à la conception ou à la mise en œuvre d'un système d'information ou à son environnement, qui pourrait être exploitée par une auteure ou un auteur de menace en vue de compromettre les biens ou les activités d'une organisation.

11.3 Références

Numéro	Référence
1	Centre canadien pour la cybersécurité. ITSG-33 Gestion des risques liés à la sécurité des TI : Une méthode axée sur le cycle de vie, décembre 2014.
2	National Institute of Standards and Technology. NIST Cybersecurity Framework.
3	International Organization for Standardization. Information technology – Security techniques – Information security management systems – Requirements, ISO/IEC 27001:2013.

Numéro	Référence
4	Centre canadien pour la cybersécurité. Contrôles de cybersécurité de base pour les petites et moyennes organisations, février 2020.
5	International Association of IT Asset Managers. IAITAM | International Association of Information Technology Managers Official Home Page
6	Centre canadien pour la cybersécurité. Nettoyage des supports de TI (ITSP.40.006), juillet 2017.
7	Secrétariat du Conseil du Trésor du Canada. Directive sur la gestion du matériel, mai 2021.
8	National Cyber Security Centre. Device Security Guidance, juin 2021.
9	Centre canadien pour la cybersécurité. Produits obsolètes (ITSAP.00.095), mars 2023.
10	International Organization for Standardization. ISO 55001:2014 is the International Standard for Asset Management, juillet 2014.
11	National Institute of Standards and Technology. NIST special publication1800-5: IT Asset Management, septembre 2018.
12	Commissariat à la protection de la vie privée du Canada. La *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE).
13	Centre canadien pour la cybersécurité. Processus d'évaluation de la sécurité des technologies de l'information s'appliquant aux fournisseurs de services infonuagiques (ITSM.50.100), octobre 2018.
14	Centre canadien pour la cybersécurité. Gérer les risques liés aux données du gouvernement du Canada dans le contexte des services infonuagiques (ITSM.50.109), août 2022.

Annexe A Catalogue des contrôles de sécurité de l'ITSG-33

A.1 Contrôle de sécurité opérationnel : Gestion des configurations (CM pour *Configuration Management*)

Le tableau 1 décrit le contrôle **CM-8 Inventaire des composants de système d'information**, tel qu'il est décrit à l'annexe 3A de l'ITSG-33 [1].

Tableau 1 : Contrôle de sécurité opérationnel CM-8 de l'ITSG-33

Numéro	Contrôle	Exigence	Améliorations du contrôle	Contrôles de l'ITSG-33 connexes
CM-8	Inventaire des composants de système d'information	(A) L'organisation élabore et tient un inventaire des composants de système d'information qui illustre exactement le système d'information actuel. (B) L'organisation élabore et tient un inventaire des composants de système d'information qui contient tous les composants se trouvant à l'intérieur de la limite d'autorisation du système d'information. (C) L'organisation élabore et tient un inventaire des composants de système d'information qui est au niveau de granularité jugé nécessaire aux fins de suivi et de production de rapports. (D) L'organisation élabore et tient un inventaire	**Mises à jour durant les installations et les retraits :** L'organisation met à jour l'inventaire des composants de système d'information lorsqu'elle installe ou retire des composants et met à jour le système d'information. **Automatisation de la maintenance :** L'organisation utilise des mécanismes automatisés pour faciliter la tenue d'un inventaire des composants du système d'information qui soit à jour, complet, exact et facilement accessible. Contrôle connexe : SI-7. **Détection automatisée de composants non autorisés :** (a) L'organisation utilise des mécanismes automatisés [*Affectation : fréquence définie par l'organisation*] pour détecter la présence de composants matériels, logiciels et micrologiciels non autorisés dans le système d'information. (b) L'organisation prend les mesures suivantes lorsqu'elle détecte des composants non autorisés : [*Sélection (un choix ou plus) : désactiver l'accès réseau de ces composants; isoler les composants; aviser [Affectation : liste des employés ou des rôles définie par l'organisation]*]. Contrôles connexes : AC-17, AC-18, AC-19, CA-7, SI-3, SI-4, SI-7, RA-5	CM-2 CM-6

		des composants de système d'information qui comprend [*Affectation : information définie par l'organisation et jugée nécessaire à la comptabilisation efficace des composants de système d'information*]. (E) L'organisation examine et met à jour l'inventaire des composants de système d'information [*Affectation : fréquence définie par l'organisation*].	**Information sur la comptabilisation :** L'organisation inclut dans l'information liée à l'inventaire de composants de système d'information une façon d'identifier par [*Sélection (un choix ou plus) : nom; poste; rôle*] les personnes responsables de l'administration de ces composants. **Aucune comptabilisation en double des composants :** L'organisation s'assure que tous les composants respectant la limite d'autorisation du système d'information ne sont pas reproduits dans d'autres inventaires de composants de système d'information. **Configurations évaluées et écarts approuvés :** L'organisation inclut dans l'inventaire des composants du système d'information les configurations de composants évaluées et les écarts approuvés en ce qui a trait aux configurations déjà déployées. Contrôles connexes : CM-2, CM-6 **Dépôt centralisé :** L'organisation fournit un dépôt centralisé contenant l'inventaire des composants de système d'information. **Localisation automatisée :** L'organisation utilise des mécanismes automatisés pour géolocaliser les composants de système d'information. **Attribution de composants à des systèmes :** (a) L'organisation attribue [*Affectation : composants de système d'information définis par l'organisation*] à un système d'information. (b) L'organisation reçoit un avis concernant cette attribution de la part du propriétaire du système d'information. Contrôle connexe : SA-4	

A.2 Contrôle de sécurité opérationnel : Protection physique et environnementale (PE pour *Physical and Environmental Protection*)

Le tableau 2 décrit le contrôle **PE-20 Surveillance et suivi des biens**, tel qu'il est décrit à l'annexe 3A de l'ITSG-33 [1].

Tableau 2 : Contrôle de sécurité opérationnel PE-20 de l'ITSG-33

Numéro	Contrôle	Exigence	Améliorations du contrôle	Contrôles de l'ITSG-33 connexes
PE-20	Surveillance et suivi des biens	(A) L'organisation utilise des [*Affectation : technologies de localisation des biens définies par l'organisation*] pour repérer et surveiller l'emplacement et le mouvement des [*Affectation : biens définis par l'organisation*] dans les [*Affectation : les secteurs contrôlés et définis par l'organisation*]. (B) L'organisation s'assure d'utiliser les technologies de localisation conformément aux lois du GC, aux politiques, directives et normes applicables du SCT.	Aucune	CM-8

A.3 Contrôle de sécurité opérationnel : Maintenance (MA)

Le tableau 3 décrit les contrôles **MA-2 Maintenance contrôlée** et **MA-6 Maintenance opportune**, tels qu'ils sont décrits à l'annexe 3A de l'ITSG-33 [1].

Tableau 3 : Contrôles de sécurité opérationnels MA-2 et MA-6 de l'ITSG-33

Numéro	Contrôle	Exigence	Améliorations du contrôle	Contrôles de l'ITSG-33 connexes
MA-2	Maintenance contrôlée	(A) L'organisation planifie, exécute, documente et examine les dossiers de maintenance et de réparation des composants de système d'information conformément aux spécifications du fabricant ou du fournisseur ou à ses propres exigences. (B) L'organisation approuve et surveille toutes les activités de maintenance, qu'elles soient effectuées sur place ou à distance et que l'équipement soit réparé sur les lieux ou dans un autre emplacement. (C) L'organisation exige que [*Affectation : personnel ou rôles définis par l'organisation*] approuve explicitement le retrait du système d'information, ou de ses composants, de ses installations aux fins de maintenance ou de réparation à l'extérieur de ses locaux. (D) L'organisation nettoie l'équipement afin de supprimer toutes les données des supports connexes avant de l'expédier à l'extérieur aux fins de maintenance ou de réparation. (E) L'organisation vérifie tous les contrôles de sécurité potentiellement concernés pour s'assurer qu'ils continuent de fonctionner adéquatement après les activités de maintenance ou de réparation. (F) L'organisation inclut [*Affectation : information portant sur la maintenance définie par*	**Activités de maintenance automatisées :** (a) L'organisation utilise des mécanismes automatisés pour planifier, exécuter et consigner les maintenances et les réparations. (b) L'organisation tient à jour des dossiers précis et complets de toutes les maintenances et réparations exigées, planifiées, en cours et exécutées. Contrôles connexes : CA-7, MA-3.	CM-3 CM-4 MA-4 MP-6 PE-16 SA-12 SI-2

Numéro	Contrôle	Exigence	Améliorations du contrôle	Contrôles de l'ITSG-33 connexes
		l'organisation] dans les dossiers de maintenance organisationnels.		
MA-6	Maintenance opportune	(A) L'organisation obtient des services de maintenance et/ou des pièces de rechange pour les [*Affectation : composants du système d'information définis par l'organisation*] dans les [*Affectation : durée définie par l'organisation*] qui suivent la panne.	**Maintenance préventive :** L'organisation effectue la maintenance préventive des [*Affectation : composants du système d'information définis par l'organisation*] tous les [*Affectation : intervalles définis par l'organisation*]. **Maintenance prévisionnelle :** L'organisation effectue la maintenance prévisionnelle des [*Affectation : composants du système d'information définis par l'organisation*] tous les [*Affectation : intervalles définis par l'organisation*]. **Soutien automatisé pour la maintenance prévisionnelle :** L'organisation utilise des mécanismes automatisés pour transférer les données de maintenance prévisionnelle à un système informatisé de gestion des activités de maintenance.	CM-8 CP-2 CP-7 SA-14 SA-15

A.4 Contrôle de sécurité de gestion : Évaluation des risques (RA pour *Risk Assessment*)

Le tableau 4 décrit le contrôle **RA-2 Catégorisation de sécurité**, tel qu'il est décrit à l'annexe 3A de l'ITSG-33 [1].

Tableau 4 : Contrôle de sécurité de gestion RA-2 de l'ITSG-33

Numéro	Contrôle	Exigence	Améliorations du contrôle	Contrôles de l'ITSG-33 connexes
RA-2	Catégorisation de sécurité	(A) L'organisation catégorise l'information et les systèmes d'information conformément aux lois du GC et aux prescriptions du SCT. (B) L'organisation documente les résultats de la catégorisation (y compris les justifications) dans le plan de sécurité du système d'information. (C) L'organisation s'assure que la décision concernant la catégorisation de sécurité est examinée et approuvée par l'autorité responsable ou par son représentant désigné.	Aucune	CM-8 MP-4 RA-3 SC-7.

A.5 Contrôle de sécurité technique : Vérification et responsabilisation (AU pour *Audit and Accountability*)

Le tableau 5 décrit les contrôles **AU-6 Examen, analyse et rapports de vérification et AU-7 Réduction des vérifications et génération de rapports**, tels qu'ils sont décrits à l'annexe 3A de l'ITSG-33 [1].

Tableau 5 : Contrôles de sécurité techniques AU-6 et AU-7 de l'ITSG-33

Numéro	Contrôle	Exigence	Améliorations du contrôle	Contrôles de l'ITSG-33 connexes
AU-6	Examen, analyse et rapports de vérification	(A) L'organisation examine et analyse les enregistrements de vérification du système d'information [*Affectation : fréquence définie par l'organisation*] pour déceler toute indication de [*Affectation : activités inappropriées ou inhabituelles définies par l'organisation*]. (B) L'organisation fait part de ses constatations à [*Affectation : liste des employés ou des rôles définie par l'organisation*].	**Intégration des processus :** L'organisation utilise des mécanismes automatisés pour intégrer les processus d'examen, d'analyse et de rapports de vérification afin de soutenir les processus organisationnels d'enquête et d'intervention en cas d'activités suspectes. Contrôle connexe : AU-12 **Dépôts de vérification correspondants :** L'organisation analyse et fait correspondre les enregistrements de vérification des différents dépôts afin d'acquérir une connaissance globale de la situation. Contrôles connexes : AU-12, IR-4 **Analyses et examens centralisés :** Le système d'information permet de centraliser les examens et les analyses des enregistrements de vérification provenant de plusieurs composants du système d'information. Contrôles connexes : AU-2, AU-12 **Intégration des capacités d'analyse et de surveillance :** L'organisation intègre l'analyse des enregistrements de vérification et l'analyse de [*Sélection (un choix ou plus) : l'information liée au balayage des vulnérabilités; les données de rendement; l'information sur la surveillance du système d'information; [Affectation : données ou information recueillies par d'autres sources définies par l'organisation]*] pour accroître sa capacité de détecter les activités inappropriées ou inhabituelles. Contrôles connexes : AU-12, IR-4, RA-5 **Opérations autorisées :** L'organisation précise les opérations qui sont autorisées concernant chaque [*Sélection (un choix ou*	AC-2 AC-3 AC-6 AC-17 AT-3 AU-7 AU-16 CA-7 CM-5 CM-10 CM-11 IA-3 IA-5 IR-5 IR-6 MA-4 MP-4 PE-3 PE-6 PE-14 PE-16 RA-5 SC-7 SC-18 SC-19 SI-3 SI-4 SI-7

Numéro	Contrôle	Exigence	Améliorations du contrôle	Contrôles de l'ITSG-33 connexes
			plus) : processus, rôle ou utilisateur] associé à l'examen, à l'analyse et aux rapports de l'information de vérification. **Analyse plein texte des commandes privilégiées :** L'organisation mène une analyse plein texte des commandes privilégiées vérifiées dans un composant de système d'information ou un sous-système physiquement distinct du système d'information ou dans un autre système d'information conçu pour mener cette analyse. Contrôles connexes : AU-3, AU-9, AU-11, AU-1 **Corrélation avec l'information provenant de sources non techniques :** L'organisation met en corrélation l'information provenant de sources non techniques et l'information de vérification afin d'acquérir une connaissance globale de sa situation. Contrôle connexe : AT-2 **Ajustement du niveau d'examen :** L'organisation ajuste le niveau d'examen, d'analyse et de rapports de vérification dans le système d'information lorsqu'un changement fondé sur des renseignements relatifs au maintien de l'ordre, du renseignement brut ou d'autres sources crédibles d'information est apporté au risque.	

Numéro	Contrôle	Exigence	Améliorations du contrôle	Contrôles de l'ITSG-33 connexes
AU-7	Réduction des vérifications et génération de rapports	(A) Le système d'information permet de réduire les vérifications et de générer des rapports pour répondre aux besoins d'examen, d'analyse et de rapports de vérification sur demande ainsi qu'aux enquêtes après coup sur les incidents de sécurité. (B) Le système d'information offre une capacité qui permet de réduire les vérifications et de générer des rapports et qui ne change pas le contenu original ni le classement chronologique des enregistrements de vérification.	**Traitement automatisé :** Le système d'information permet de traiter des enregistrements de vérification liés à des événements d'intérêt selon [*Affectation : champs d'enregistrements de vérification définis par l'organisation*]. Contrôles connexes : AU-2, AU-12 **Triage et recherche automatisés :** Le système d'information permet de trier et de rechercher des enregistrements de vérification liés à des événements d'intérêt selon le contenu de [*Affectation : champs des enregistrements de vérification définis par l'organisation*].	AU-6