Communications Security Establishment
Centre de la sécurité des télécommunications

Conseils en matière de sécurité des technologies de l'information

La gestion des risques liés à la sécurité des TI : Une méthode axée sur le cycle de vie

Activités de gestion des risques liés à la sécurité des systèmes d'information

ITSG-33 – Annexe 2

Novembre 2012

Canada

Avant-propos

L'Annexe 2 (*Activités de gestion des risques liés à la sécurité des systèmes d'information*) de *La gestion des risques liés à sécurité des TI : Une méthode axée sur le cycle de vie* (ITSG-33) est un document non classifié publié avec l'autorisation du chef du Centre de la sécurité des télécommunications (CST).

Les propositions de modification devraient être envoyées au représentant des Services à la clientèle de la Sécurité des TI du CST par l'intermédiaire des responsables de la sécurité des TI du ministère.

Les demandes de copies supplémentaires ou de modification de la distribution devraient être soumises au représentant des Services à la clientèle de la Sécurité des TI du CST.

Pour de plus amples renseignements, prière de communiquer avec les Services à la clientèle de la Sécurité des TI du CST, par courriel à l'adresse itsclientservices@cse-cst.gc.ca, ou par téléphone au 613-991-7654.

Date d'entrée en vigueur

Cette publication entre en vigueur le 1er novembre 2012.

La chef adjointe, Sécurité des TI,

Signé initialement par

Toni Moffa

Résumé

La présente annexe fait partie d'une suite de directives sur la gestion des risques liés à la sécurité des technologies de l'information (TI) que le Centre de la sécurité des télécommunications (CST) publie dans le numéro 33 de la série Conseils en matière de sécurité des technologies de l'information (guide ITSG-33) pour aider les ministères et organismes du gouvernement du Canada (GC) à mettre en œuvre, exploiter et maintenir des systèmes d'information fiables.

Les lignes directrices du guide ITSG-33 décrivent un processus de gestion des risques liés à la sécurité des TI qui inclut les activités menées à deux niveaux distincts : niveau du ministère et niveau du système d'information.

L'annexe propose un processus d'application de la sécurité dans les systèmes d'information (PASSI). Le but de ce processus est d'aider les responsables des projets de TI à intégrer aux systèmes d'information des solutions de sécurité qui répondent aux objectifs de confidentialité, d'intégrité et de disponibilité des activités opérationnelles prises en charge par ces systèmes. Dans la présente annexe, un projet de TI est défini comme une entreprise temporaire visant la mise en place d'un nouveau système d'information ou la mise en œuvre de changements importants apportés à un système d'information existant. Par définition, cette notion présume que chaque projet se termine lorsque le nouveau système de TI entre en fonction ou que les changements apportés au système existant sont terminés, et que l'organisation chargée de l'exploitation des TI en assume la responsabilité opérationnelle.

Le respect des lignes directrices énoncées dans le guide ITSG-33 offre de nombreux avantages aux ministères, notamment : conformité à l'ensemble de la stratégie et des objectifs de gestion des risques établis par le Secrétariat du Conseil du Trésor (SCT), approche efficace des principaux aspects de la sécurité des TI et gestion uniforme et rentable des risques liés à la sécurité des TI.

Table des matières

Liste des figures

Liste des tableaux

Liste des abréviations et des sigles

BNS	Besoins opérationnels en matière de sécurité
CDS	Cycle de développement des systèmes
CEI	Commission électrotechnique internationale
CM	Gestion de la configuration
COMSEC	Sécurité des communications
CPI	Centre de protection de l'information
CST	Centre de la sécurité des télécommunications
CVS	Cycle de vie des systèmes
DGMS	Directive sur la gestion de la sécurité ministérielle
DP	Demande de proposition
DS	Spécifications de conception
DT	Outils de développement
EM	Évaluation des menaces
EMR	Évaluation des menaces et des risques
ENS	Entente sur les niveaux de service
FIPS	Federal Information Processing Standard
GC	Gouvernement du Canada
GRC	Gendarmerie royale du Canada
IATF	Information Assurance Technical Framework
ISO	Organisation internationale de normalisation
ITSG	Conseils en matière de sécurité des technologies de l'information
LVERS	Liste de vérification des exigences relatives à la sécurité
MTES	Matrice de traçabilité des exigences de sécurité
NAS	Niveau d'assurance de la sécurité
NIST	National Institute of Standards and Technology
NSA	National Security Agency
OpenSSL	Open Secure Socket Layer
OSP	Procédures de sécurité opérationnelles
OTAN	Organisation du Traité de l'Atlantique Nord
PASSI	Processus d'application de la sécurité dans les systèmes d'information
PE	Protocole d'entente
PGSG	Politique sur la sécurité du gouvernement

PSM	Plan de sécurité ministérielle
RAD	Développement rapide d'applications
SCS	Spécification des contrôles de sécurité
SCT	Secrétariat du Conseil du Trésor
SDP	Pratiques de développement sécurisé
SIP	Procédures d'installation des composants de sécurité
SIV	Vérification de l'installation des composants de sécurité
SM	Mesures de sécurité
SPIN	Avis de mise en œuvre de la politique sur la sécurité
SPC	Services partagés Canada
SQL	Langage d'interrogation SQL
SSE-GCM	Ingénierie de sécurité des systèmes – Modèle d'évolution des capacités
SSH	Protocole SSH (Secure Shell)
SSL	Protocole SSL (Secure Socket Layer)
ST	Tests de sécurité
TCP	Protocole TCP (Transmission Control Protocol)
TI	Technologie de l'information
TLS	Protocole TLS (Transport Layer Security)
TPSGC	Travaux publics et Services gouvernementaux Canada
URL	Adresse URL (Uniform Ressource Locator)
VA	Évaluation des vulnérabilités

1 Introduction

1.1 Objet et portée

La présente annexe fournit aux ministères du gouvernement du Canada (GC)[1] des directives sur la mise en œuvre efficace et rentable de mécanismes de sécurité dans les systèmes d'information, en conformité avec les politiques, normes et lignes directrices promulguées par le Secrétariat du Conseil du Trésor du Canada (SCT). Elle traite des activités au niveau du système d'information qui s'inscrivent dans le processus de gestion des risques liés à la sécurité des technologies de l'information (TI) que les lignes directrices du guide ITSG-33 proposent aux ministères.

L'annexe propose un processus d'application de la sécurité dans les systèmes d'information (PASSI) pour les projets de TI du GC. Le but de ce processus est d'aider les responsables des projets de TI à intégrer aux systèmes d'information des solutions de sécurité qui répondent aux objectifs de confidentialité, d'intégrité et de disponibilité des activités opérationnelles ministérielles prises en charge par ces systèmes. Dans la présente annexe, un projet de TI est défini comme une entreprise temporaire visant la mise en place d'un nouveau système d'information ou la mise en œuvre de changements importants apportés à un système d'information existant. Par définition, cette notion présume que chaque projet se termine lorsque le nouveau système de TI entre en fonction ou que les changements apportés au système existant sont terminés, et que l'organisation chargée de l'exploitation des TI en assume la responsabilité opérationnelle.

Bien que cela ne fasse pas partie intégrante de son champ d'application, l'annexe inclut également des directives de nature générale sur les activités supplémentaires de gestion des risques qui suivent la mise en œuvre des systèmes, notamment la protection à la fois de l'exploitation et de la maintenance des systèmes, et celle de l'élimination des biens de TI à la fin de leur vie utile.

1.2 Champ d'application

Les lignes directrices énoncées dans cette publication concernent l'application de la sécurité dans les systèmes d'information utilisés pour soutenir les activités opérationnelles des ministères dans les domaines non classifiés, protégés et classifiés. Les ministères peuvent utiliser le PASSI :

- pour développer de nouveaux systèmes d'information ministériels et les infrastructures de TI communes partagées du GC;
- lorsqu'ils apportent des changements importants aux systèmes d'information existants et aux infrastructures de TI communes partagées du GC;
- lorsqu'ils font l'acquisition de capacités de systèmes d'information externes qui seront utilisées à titre de services de TI autonomes ou intégrées aux systèmes d'information du GC.

Les responsables d'un projet de TI font l'acquisition de capacités externes lorsqu'ils prévoient tirer un meilleur avantage d'une capacité offerte par un autre système d'information ou une autre infrastructure de TI que de celle qu'offre le projet. Les fournisseurs de ces capacités peuvent être d'autres organisations au sein du ministère parrain, d'autres ministères (p. ex., Services partagés Canada (SPC), fournisseur de services communs du GC) ou des fournisseurs de services commerciaux.

[1] Le terme *ministère* est utilisé pour désigner des ministères, organismes et autres organisations du GC assujettis à la *Politique sur la sécurité du gouvernement* [Référence 3].

La définition de ce qui constitue un changement pour les systèmes d'information existants et les infrastructures de TI communes partagées du GC est sujette à interprétation. Dans la plupart des cas, les changements apportés aux systèmes d'information, quelle que soit leur ampleur, requièrent une autorisation et une certaine évaluation de la sécurité. Les autorités ministérielles déterminent normalement au cas par cas si les changements proposés peuvent être effectués par leur propre organisation de TI à partir de procédures opérationnelles établies (p. ex., des procédures de gestion du changement qui traitent des aspects de la sécurité) ou si leur ampleur est telle qu'elle justifie l'établissement d'un projet de TI.

Le PASSI est un processus intégré et est décrit en détail dans le présent document. On s'attend à ce que les ministères qui ont des capacités d'ingénierie et de gestion de projet de TI bien établies puissent facilement adapter et intégrer le PASSI à leur propre processus de cycle de développement des systèmes (CDS). Ceux qui ne disposent pas de telles capacités ne seront pas en mesure d'appliquer immédiatement toutes les facettes du PASSI et devront procéder à une adaptation plus poussée du processus. Les responsables de projets de TI dans ces ministères peuvent utiliser le présent document comme référence pour améliorer graduellement leurs pratiques d'ingénierie de sécurité et mettre en place des systèmes d'information plus fiables.

1.3 Objectifs et résultats attendus

L'objectif de la présente annexe est d'aider les ministères à mettre en place et à exploiter des systèmes d'information fiables et appropriés, conformes aux objectifs et aux exigences de la *Politique sur la sécurité du gouvernement* (PSG) [Référence 3], de la *Directive sur la gestion de la sécurité ministérielle* (DGMS) [Référence 4], et de la *Norme opérationnelle de sécurité : Gestion de la sécurité des technologies de l'information* (GSTI) [Référence 5] du SCT.

Le respect des lignes directrices énoncées dans la présente annexe permet aux responsables des projets de TI d'obtenir les résultats suivants :

- Mettre en place ou acquérir des systèmes d'information ou des capacités qui répondent aux exigences de sécurité des activités opérationnelles ministérielles;
- Mettre en place des systèmes d'information suffisamment robustes pour résister à des menaces[2] particulières, dont les niveaux de risque sont acceptables, dans l'environnement opérationnel;
- Donner aux intervenants, qui font confiance aux systèmes d'information, un aperçu réaliste des risques auxquels sont exposées les activités opérationnelles ministérielles.

[2] Les ministères doivent préciser, pour toutes les menaces potentielles, un sous-ensemble de menaces contre lesquelles ils désirent protéger leurs biens de TI. Cela signifie que certaines menaces ont pu être cernées et envisagées, mais ont été jugées non pertinentes pour différentes raisons. Par exemple, un ministère peut juger que la protection contre une menace donnée peut s'avérer trop coûteuse ou complexe ou qu'elle peut restreindre de manière significative une fonction de soutien d'une activité opérationnelle. L'information sur les menaces, y compris les décisions et les justifications d'exclusion de menaces spécifiques, est normalement documentée dans les rapports ministériels d'évaluation des menaces. Voir l'Annexe 1 du guide ITSG-33 [Référence 1] pour en savoir plus.

1.4 Auditoire

La présente annexe concerne les participants aux différentes phases des projets de mise en œuvre des systèmes d'information. Elle inclut plus spécifiquement des directives à l'intention des autorisateurs, des gestionnaires de projet, des architectes, des praticiens et des évaluateurs de la sécurité, ainsi que des membres des groupes responsables des opérations de TI.

1.5 Conformité aux lois du GC et aux instruments de politique du SCT

Le guide ITSG-33 comprend des directives pour aider les ministères à répondre aux exigences principales des instruments de politique du SCT en matière de sécurité des TI et de gestion des risques liés à la sécurité des TI, et pour soutenir les efforts déployés par les praticiens de la sécurité pour protéger les systèmes d'information conformément aux lois applicables du GC et aux politiques, aux directives et aux normes du SCT en matière de contrôles de sécurité.

1.6 Structure de la publication

La présente annexe fait partie d'une suite de documents sur la gestion des risques liés à la sécurité des TI au sein du GC. Les autres documents sont les suivants :

- ITSG-33, Aperçu – *La gestion des risques liés à la sécurité des TI : Une méthode axée sur le cycle de vie*;
- ITSG-33, Annexe 1 – *Activités de gestion des risques liés à la sécurité des TI*;
- ITSG-33, Annexe 3 – *Catalogue des contrôles de sécurité*;
- ITSG-33, Annexe 4 – *Profils de contrôle de sécurité*;
- ITSG-33, Annexe 5 – *Glossaire*.

1.7 Définitions

Pour obtenir les définitions des principaux termes utilisés dans la présente annexe, consultez l'Annexe 5 du guide ITSG-33 [Référence 11].

2 Aperçu du processus d'application de la sécurité dans les systèmes d'information (PASSI)

2.1 Approche générale

Le PASSI est un processus intégré basé sur un ensemble structuré d'activités servant à l'application de la sécurité dans les systèmes d'information. Il inclut des activités portant sur l'ingénierie de sécurité[3], l'évaluation des menaces et des risques, l'évaluation de la sécurité et l'autorisation des systèmes d'information. La Figure 1 à la page suivante donne un aperçu du PASSI.

Pour appliquer le PASSI de manière efficace et rentable, les responsables des projets de TI doivent intégrer ses activités aux activités d'ingénierie et de test de système et aux autres activités de leur processus de CDS particulier. Pour les aider à réaliser cette intégration, le PASSI établit les correspondances entre les activités de sécurité et les différentes phases du processus de CDS de référence suivant un modèle en cascade type. Par exemple, le PASSI propose d'intégrer l'activité d'analyse des besoins de sécurité aux activités plus larges d'analyse des besoins liés au système. La même recommandation s'applique aux activités de conception, de test, d'assurance de la qualité, et à toute autre activité pertinente. Notons que le PASSI n'inclut pas toutes les activités requises pour un projet de TI; seulement celles qui concernent la sécurité des TI sont indiquées.

Les gestionnaires de projets de TI peuvent adapter le PASSI aux autres méthodologies de CDS, par exemple celles qui utilisent des processus allégés, comme la méthode Agile et d'autres méthodologies RAD (développement rapide d'applications). Les directives portant sur l'adaptation des activités du PASSI à d'autres méthodologies de CDS, telles celles mentionnées ci-dessus, débordent du cadre des documents de l'ITSG-33. Comme illustré dans la Figure 1, le modèle de référence CDS inclut les phases suivantes :

- **Mobilisation des intervenants** – Identifier et motiver les intervenants du projet de TI;
- **Concept** – Définir un concept pour le système d'information;
- **Planification** – Planifier la mise en œuvre du système d'information;
- **Analyse des besoins** – Définir les exigences dont le système d'information doit tenir compte pour répondre aux objectifs opérationnels;
- **Conception de haut niveau** – Créer une conception de système de haut niveau qui répond aux exigences du système d'information;
- **Conception détaillée** – Préciser une conception détaillée pour la conception de système de haut niveau;
- **Développement** – Développer ou acquérir et tester les composants individuels du système d'information;
- **Intégration et test** – Intégrer les composants individuels dans un système complet et effectuer un test d'intégration;
- **Installation** – Installer le système d'information dans l'environnement de production.

[3] Le PASSI traite des différents domaines de traitement définis dans le document *Information Technology – Systems Security Engineering – Capability Maturity Model* (SSE-CMM) de l'ISO/IEC [Référence 6].

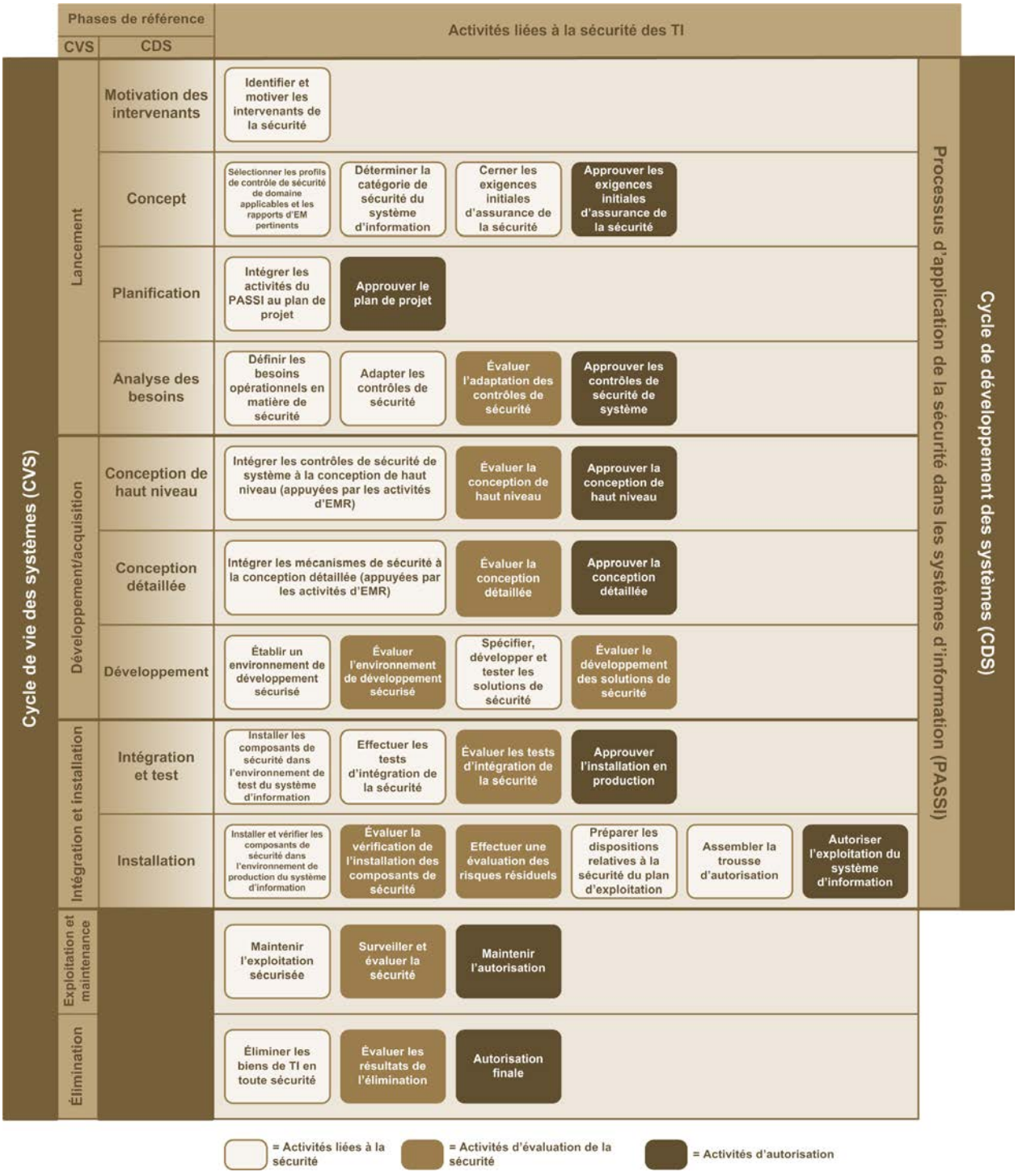


Figure 1 : Aperçu du PASSI

La Figure 1 inclut deux phases supplémentaires en plus de celles du CDS afin d'illustrer tout le cycle de vie des systèmes (CVS) :

- **Exploitation et maintenance** – Un groupe responsable des opérations de TI exploite et tient à jour le système d'information jusqu'à la fin de sa vie utile;
- **Élimination** – Au moment du retrait du système à la fin de sa vie utile, le groupe responsable des opérations de TI élimine ou attribue de nouveau les biens de TI.

Cette description du CDS de référence est générique et traite de tous les aspects des TI, tels le rendement, la fiabilité, la convivialité et la sécurité. Dans un CDS type, ces aspects sont pris en compte à chaque phase et intégrés à chacune : analyse des besoins qui tient compte de tous les besoins, activités de conception qui visent à répondre à toutes les exigences, etc. À des fins d'efficacité, les différents aspects des TI ne sont pas gérés de manière indépendante, tout comme les aspects liés à la sécurité des systèmes d'information. Les activités qui concernent la sécurité sont intégrées aux activités du CDS type et menées en intégration avec ces dernières. Cela permet d'accroître l'efficacité du processus et la confiance dans le traitement adéquat de tous aspects liés à la sécurité.

La progression des objectifs de sécurité vers l'application des solutions de sécurité dans le système d'information comporte plusieurs stades de spécifications de sécurité de plus en plus détaillées, qui incluent les besoins opérationnels en matière de sécurité (p. ex., voir à ce que l'information sur les transactions administratives ne soit pas divulguée à des parties non autorisées), les contrôles de sécurité de système (p. ex., la confidentialité des transmissions), les mécanismes de sécurité (p. ex., le chiffrement des sessions TLS [Transport Layer Security]) et, finalement, les solutions de sécurité intégrées au système d'information (p. ex., OpenSSL Version 3) qui seront ensuite installées dans l'environnement du système d'information.

Notons que la phase d'exploitation et de maintenance et la phase d'élimination ne font pas partie à proprement parler du CDS; elles sont indiquées pour souligner l'importance des liens entre la mise en œuvre sécurisée des systèmes d'information et la sécurisation de leurs processus d'exploitation, de maintenance et d'élimination. Des directives concernant ces phases sont énoncées aux sections 4 et 5.

2.2 Avantages de l'utilisation du PASSI

En respectant les lignes directrices énoncées dans la présente annexe, les ministères sont en mesure :

- de se conformer aux principaux instruments promulgués par le SCT en matière de sécurité des TI et de gestion des risques liés à la sécurité des TI;
- de tirer avantage d'une approche globale pour répondre aux préoccupations que soulève la sécurité des TI au chapitre de la mise en œuvre et de l'exploitation des systèmes d'information;
- de mettre en place de manière uniforme et rentable des systèmes d'information fiables qui répondent aux objectifs opérationnels et aux besoins de sécurité.

2.3 Conditions d'autorisation

Avant le lancement d'un projet de TI, le gestionnaire de projet doit consulter le plan de sécurité ministérielle (PSM) et prendre connaissance de la liste des conditions minimales qui doivent être respectées pour obtenir l'autorisation de passer à l'étape d'exploitation et de maintenance continues du

système d'information. Si ces conditions ne sont pas documentées dans le PSM, il doit les obtenir de l'autorisateur désigné. Il doit ensuite documenter la liste dans une charte de projet ou dans le plan de projet. La charte ou le plan doivent ensuite être signés par l'autorisateur, le parrain du projet de TI (s'il est différent), le gestionnaire de projet de TI et tout autre intervenant concerné, telle l'autorité opérationnelle chargée du système d'information.

Dans le contexte du PASSI, les conditions d'autorisation peuvent inclure les éléments suivants :

- Le projet de TI doit utiliser un profil de contrôle de sécurité ministériel ou de domaine;
- Les activités du PASSI doivent être adaptées et intégrées de manière appropriée au plan de projet de TI;
- Les extrants du PASSI doivent être remis à l'évaluateur de la sécurité et à l'autorisateur aux fins d'évaluation et d'approbation, en conformité avec les activités d'évaluation et d'approbation du PASSI;
- Une trousse d'autorisation convenue doit être préparée et remise à l'autorisateur, qui doit l'approuver avant le début des activités d'exploitation;
- Un plan d'exploitation, qui inclut des dispositions relatives à la sécurité, doit être produit et mis en œuvre par le groupe responsable des opérations de TI;
- Le niveau acceptable de risque résiduel du système d'information doit être faible.

3 Description du PASSI

Ce chapitre décrit les activités du PASSI correspondant aux neuf phases du cycle de développement des systèmes (CDS) de référence. Chaque sous-section suivante décrit une phase du CDS de référence et inclut une ou plusieurs sous-sections, chacune décrivant les activités du PASSI menées à bien au cours de cette phase. Dans cette section, les extrants du PASSI sont identifiés par le numéro de sous-section pertinent (correspondant à l'activité dont ils résultent) et des identificateurs alphabétiques.

Les activités du PASSI sont décrites selon une structure uniforme qui comprend les éléments suivants :

- **Objectif** – Objectif de l'activité;
- **Rôle principal** – Rôle de la personne chargée de mener à bien l'activité;
- **Rôles de soutien** – Rôles qui appuient les rôles principaux et leur permettent de mener à bien l'activité;
- **Intrants** – Intrants de l'activité;
- **Extrants** – Extrants de l'activité;
- **Exigences d'assurance de la sécurité** – Identificateurs et titres des exigences d'assurance de la sécurité qui s'appliquent à l'activité (voir les descriptions à la section 8);
- **Lignes directrices** – Lignes directrices sur la façon de mener à bien l'activité.

Bien que les activités du PASSI soient décrites séquentiellement dans la présente annexe, aucun processus n'est complètement linéaire. Il peut arriver fréquemment durant un projet que l'équipe responsable doive revenir à une activité précédente, même à une phase antérieure, pour terminer ou refaire une partie d'une analyse ou raffiner des définitions et des spécifications. Il convient de noter également que le PASSI n'exclut pas le besoin de recourir à des points de contrôle standard du CDS et à des approbations de la direction, tels des examens critiques de la conception et des points de contrôle de la qualité.

Le Tableau 1 résume le processus et inclut une liste de toutes les activités du PASSI avec leurs intrants et leurs extrants. Les extrants indiqués dans la dernière colonne représentent des produits associés aux travaux du PASSI et non nécessairement des produits livrables ou des documents individuels. Afin de réduire la taille de la documentation, les responsables des projets de TI doivent, dans la mesure du possible, inclure les extrants du PASSI dans les produits livrables habituels du CDS (p. ex., intégrer les exigences de sécurité aux spécifications des exigences du système, aux conceptions de la sécurité, aux documents de conception du système, etc.) déterminés durant la phase de planification. À cette fin, le Tableau 2 donne la liste de tous les produits associés aux travaux du PASSI et propose des produits livrables du CDS auxquels ils peuvent être intégrés.

Le Tableau 3 propose des suggestions d'attribution d'activités du PASSI aux rôles principaux et de soutien. Les responsabilités de ces rôles dans le contexte du PASSI sont décrites à l'Annexe 1 du guide ITSG-33 [Référence 1].

Tableau 1 : Activités, intrants et extrants du PASSI

Sous-sections	Activités	Intrants	Extrants
3.1	**Phase de motivation des intervenants**		
3.1.1	Identifier et motiver les intervenants de la sécurité	ITSG-33, Annexe 2 – *Activités de gestion des risques liés à la sécurité des systèmes d'information* [le présent document] Documentation de projet existante	(3.1.1-A) Liste des intervenants de la sécurité
3.2	**Phase de concept**		
3.2.1	Sélectionner les profils de contrôle de sécurité de domaine et les rapports d'évaluation des menaces applicables	Documentation de projet existante Profils de contrôle de sécurité de domaine existants Rapports d'évaluation des menaces de domaine existants	(3.2.1-A) Profils de contrôle de sécurité de domaine applicables (3.2.1-B) Rapports d'évaluation de menaces de domaine pertinents
3.2.2	Déterminer la catégorie de sécurité du système d'information	ITSG-33, Annexe 1, section 7 – *Processus de catégorisation de la sécurité* [Référence 1] (3.2.1-A) Profils de contrôle de sécurité de domaine applicables	(3.2.2-A) Rapport sur la catégorisation de la sécurité du système d'information
3.2.3	Cerner les exigences initiales d'assurance de la sécurité	ITSG-33, Annexe 2, section 8 – *Exigences d'assurance de la sécurité* [le présent document] (3.2.1-A) Profils de contrôle de sécurité de domaine applicables (3.2.1-B) Rapports d'évaluation des menaces de domaine pertinents (3.2.2-A) Rapport sur la catégorisation de la sécurité du système d'information	(3.2.3-A) Exigences initiales d'assurance de la sécurité
3.2.4	Approuver les exigences initiales d'assurance de la sécurité	(3.2.3-A) Exigences initiales d'assurance de la sécurité	(3.2.4-A) Exigences initiales d'assurance de la sécurité approuvées
3.3	**Phase de planification**		
3.3.1	Intégrer les activités du PASSI au plan de projet	Plan de projet ITSG-33, Annexe 2 – *Activités de gestion des risques liés à la sécurité des systèmes d'information* [le présent document] (3.1.1-A) Liste des intervenants de la sécurité (3.2.4-A) Exigences initiales d'assurance de la sécurité approuvées	(3.3.1-A) Plan de projet incluant les activités du PASSI

Sous-sections	Activités	Intrants	Extrants
3.3.2	Approuver le plan de projet	(3.3.1-A) Plan de projet incluant les activités du PASSI	(3.3.2-A) Plan de projet approuvé incluant les activités du PASSI
3.4	**Phase d'analyse des besoins**		
3.4.1	Définir les besoins opérationnels en matière de sécurité	Documentation du système de la phase de concept (3.2.1-A) Profils de contrôle de sécurité de domaine applicables (3.2.2-A) Rapport sur la catégorisation de la sécurité du système d'information (3.2.4-A) Exigences initiales d'assurance de la sécurité approuvées	(3.4.1-A) Besoins opérationnels en matière de sécurité
3.4.2	Adapter les contrôles de sécurité	ITSG-33, Annexe 3 – *Catalogue des contrôles de sécurité* [Référence 7] Documentation système de la phase de concept (3.2.1-A) Profils de contrôle de sécurité de domaine applicables (3.2.2-A) Rapport sur la catégorisation de la sécurité du système d'information (3.2.4-A) Exigences initiales d'assurance de la sécurité approuvées (3.4.1-A) Besoins opérationnels en matière de sécurité	(3.4.2-A) Contrôles de sécurité de système
3.4.3	Évaluer l'adaptation des contrôles de sécurité	(3.2.1-A) Profils de contrôle de sécurité de domaine applicables (3.2.4-A) Exigences initiales d'assurance de la sécurité approuvées (3.4.1-A) Besoins opérationnels en matière de sécurité (3.4.2-A) Contrôles de sécurité de système	(3.4.3-A) Énoncé d'évaluation de l'adaptation des contrôles de sécurité
3.4.4	Approuver les contrôles de sécurité de système	(3.4.2-A) Contrôles de sécurité de système (3.4.3-A) Énoncé d'évaluation de l'adaptation des contrôles de sécurité	(3.4.4-A) Contrôles de sécurité de système approuvés

Sous-sections	Activités	Intrants	Extrants
3.5	**Phase de conception de haut niveau**		
3.5.1	Intégrer les contrôles de sécurité de système à la conception de haut niveau (appuyées par les activités d'EMR)	ITSG-33, Annexe 3 – *Catalogue des contrôles de sécurité* [Référence 7] ITSG-33, Annexe 2, section 7 – *Déterminer le niveau de robustesse* [le présent document] Publications de l'ITSG sur la conception des contrôles de sécurité (3.2.1-B) Rapports d'évaluation des menaces de domaine pertinents (3.2.2-A) Rapport sur la catégorisation de la sécurité du système d'information (3.2.4-A) Exigences initiales d'assurance de la sécurité approuvées (3.4.4-A) Contrôles de sécurité de système approuvés	(3.5.1-A) Spécifications de la conception de système de haut niveau, incluant les contrôles de sécurité (3.5.1-B) Contrôles de sécurité de système révisés (3.5.1-C) Résultats des activités d'EMR
3.5.2	Évaluer la conception de haut niveau	(3.2.4-A) Exigences initiales d'assurance de la sécurité approuvées (3.5.1-A) Spécifications de la conception de système de haut niveau, incluant les contrôles de sécurité (3.5.1-B) Contrôles de sécurité de système révisés (3.5.1-C) Résultats des activités d'EMR	(3.5.2-A) Énoncé d'évaluation de la conception de système de haut niveau
3.5.3	Approuver la conception de haut niveau	(3.5.1-A) Spécifications de la conception de système de haut niveau, incluant les contrôles de sécurité (3.5.2-A) Énoncé d'évaluation de la conception de système de haut niveau	(3.5.3-A) Spécifications de la conception de système de haut niveau approuvées, incluant les contrôles de sécurité

Sous-sections	Activités	Intrants	Extrants
3.6	**Phase de conception détaillée**		
3.6.1	Intégrer les mécanismes de sécurité à la conception détaillée (appuyées par les activités d'EMR)	ITSG-33, Annexe 3 – *Catalogue des contrôles de sécurité* [Référence 7] ITSG-33, Annexe 2, section 7 – *Déterminer le niveau de robustesse* [le présent document] Publications sur la conception des contrôles de sécurité de la série ITSG Normes de sécurité technique et meilleures pratiques du gouvernement et de l'industrie (3.2.2-A) Rapport sur la catégorisation de la sécurité du système d'information (3.2.4-A) Exigences initiales d'assurance de la sécurité approuvées (3.5.1-B) Contrôles de sécurité de système révisés (3.5.1-C) Résultats des activités d'EMR (3.5.3-A) Spécifications de la conception de système de haut niveau approuvées, incluant les contrôles de sécurité	(3.6.1-A) Spécifications de la conception de système détaillée, incluant les mécanismes de sécurité (3.6.1-B) Version définitive des contrôles de sécurité de système (3.6.1-C) Exigences d'assurance de la sécurité à jour (3.6.1-D) Résultats des activités d'EMR
3.6.2	Évaluer la conception détaillée	(3.6.1-A) Spécifications de la conception de système détaillée, incluant les mécanismes de sécurité (3.6.1-B) Version définitive des contrôles de sécurité de système (3.6.1-C) Exigences d'assurance de la sécurité à jour (3.6.1-D) Résultats des activités d'EMR	(3.6.2-A) Énoncé d'évaluation de la conception de système détaillée

Sous-sections	Activités	Intrants	Extrants
3.6.3	Approuver la conception détaillée et le développement	(3.6.1-A) Spécifications de la conception de système détaillée, incluant les mécanismes de sécurité (3.6.2-A) Énoncé d'évaluation de la conception de système détaillée	(3.6.3-A) Spécifications approuvées de la conception de système détaillée, incluant les mécanismes de sécurité (3.6.3-B) Autorisation de commencer la phase de développement
3.7	**Phase de développement**		
3.7.1	Établir un environnement de développement sécurisé	(3.6.1-C) Exigences d'assurance de la sécurité à jour (3.6.3-A) Spécifications approuvées de la conception de système détaillée, incluant les mécanismes de sécurité (3.6.3-B) Autorisation de commencer la phase de développement	(3.7.1-A) Environnement de développement sécurisé (3.7.1-B) Documentation de l'environnement de développement
3.7.2	Évaluer l'environnement de développement sécurisé	(3.6.1-C) Exigences d'assurance de la sécurité à jour (3.7.1-A) Environnement de développement sécurisé (3.7.1-B) Documentation de l'environnement de développement	(3.7.2-A) Énoncé d'évaluation de l'environnement de développement sécurisé
3.7.3	Préciser, développer et tester les solutions de sécurité	Normes techniques de configuration de la sécurité et meilleures pratiques (3.6.1-C) Exigences d'assurance de la sécurité à jour (3.6.3-A) Spécifications approuvées de la conception de système détaillée, incluant les mécanismes de sécurité (3.7.1-A) Environnement de développement sécurisé (3.7.1-B) Documentation de l'environnement de développement	(3.7.3-A) Représentation de la mise en œuvre du système d'information, incluant la sécurité (3.7.3-B) Plans, scénarios et résultats des tests de la sécurité du développement (3.7.3-C) Procédures de sécurité opérationnelles (3.7.3-D) Procédures d'installation des composants de sécurité

Sous-sections	Activités	Intrants	Extrants
3.7.4	Évaluer le développement des solutions de sécurité	(3.6.1-C) Exigences d'assurance de la sécurité à jour (3.7.3-A) Représentation de la mise en œuvre du système d'information, incluant la sécurité (3.7.3-B) Plans, scénarios et résultats des tests de la sécurité du développement (3.7.3-C) Procédures de sécurité opérationnelles (3.7.3-D) Procédures d'installation des composants de sécurité	(3.7.4-A) Énoncé d'évaluation du développement de la sécurité
3.8	**Phase d'intégration et de test**		
3.8.1	Installer les composants de sécurité dans l'environnement de test du système d'information	(3.7.3-A) Représentation de la mise en œuvre du système d'information, incluant la sécurité	(3.8.1-A) Environnement de test du système d'information, incluant la sécurité
3.8.2	Effectuer les tests d'intégration de la sécurité	(3.6.1-C) Exigences d'assurance de la sécurité à jour (3.7.3-A) Représentation de la mise en œuvre du système d'information, incluant la sécurité (3.8.1-A) Environnement de test du système d'information, incluant la sécurité	(3.8.2-A) Plans, scénarios et résultats des tests d'intégration de la sécurité
3.8.3	Évaluer les tests d'intégration de la sécurité	(3.6.1-C) Exigences d'assurance de la sécurité à jour (3.8.1-A) Environnement de test du système d'information, incluant la sécurité (3.8.2-A) Plans, scénarios et résultats des tests d'intégration de la sécurité	(3.8.3-A) Énoncé d'évaluation des tests d'intégration de la sécurité

Sous-sections	Activités	Intrants	Extrants
3.8.4	Approuver l'installation en production	(3.7.2-A) Énoncé d'évaluation de l'environnement de développement sécurisé (3.7.4-A) Énoncé d'évaluation du développement de la sécurité (3.8.3-A) Énoncé d'évaluation des tests d'intégration de la sécurité	(3.8.4-A) Autorisation de commencer la phase d'installation en production
3.9	**Phase d'installation**		
3.9.1	Installer et vérifier les composants de sécurité du système d'information dans l'environnement de production	(3.6.1-C) Exigences d'assurance de la sécurité à jour (3.7.3-A) Représentation de la mise en œuvre du système d'information, incluant la sécurité (3.8.4-A) Autorisation de commencer la phase d'installation en production	(3.9.1-A) Environnement de production du système d'information, incluant la sécurité (3.9.1-B) Résultats de la vérification de l'installation des composants de sécurité
3.9.2	Évaluer la vérification de l'installation des composants de sécurité	(3.6.1-C) Exigences d'assurance de la sécurité à jour (3.7.3-A) Représentation de la mise en œuvre du système d'information, incluant la sécurité (3.9.1-A) Environnement de production du système d'information, incluant la sécurité (3.9.1-B) Résultats de la vérification de l'installation des composants de sécurité	(3.9.2-A) Énoncé d'évaluation de la vérification de l'installation des composants de sécurité
3.9.3	Effectuer une évaluation des risques résiduels	Tous les extrants précédents du PASSI	(3.9.3-A) Résultats de l'évaluation des risques résiduels
3.9.4	Préparer les dispositions relatives à la sécurité du plan d'exploitation	Tous les extrants précédents du PASSI	(3.9.4-A) Dispositions relatives à la sécurité du plan d'exploitation
3.9.5	Assembler la trousse d'autorisation	Tous les extrants précédents du PASSI	(3.9.5-A) Trousse d'autorisation
3.9.6	Autoriser l'exploitation du système d'information	(3.9.5-A) Trousse d'autorisation	(3.9.6-A) Autorisation de passer à l'étape d'exploitation

Tableau 2 : Intégration proposée des extrants du PASSI dans les produits livrables de projet de TI

N° d'identification	Extrants du PASSI	Produits livrables de projet de TI proposés
3.1.1-A	Liste des intervenants de la sécurité	Charte de projet
3.2.1-A	Profils de contrôle de sécurité de domaine applicables	Sans objet. Produit livrable associé aux activités de gestion des risques liés à la sécurité des TI
3.2.1-B	Rapports d'évaluation de menaces de domaine pertinents	Sans objet. Produit livrable associé aux activités de gestion des risques liés à la sécurité des TI
3.2.2-A	Rapport sur la catégorisation de la sécurité du système d'information	Sans objet. Document autonome
3.2.3-A	Exigences initiales d'assurance de la sécurité	• Plan d'assurance de la qualité • Calendrier de projet
3.2.4-A	Exigences initiales d'assurance de la sécurité approuvées	
3.6.1-C	Exigences d'assurance de la sécurité à jour	
3.3.1-A	Plan de projet incluant les activités du PASSI	Plan de projet
3.3.2-A	Plan de projet approuvé incluant les activités du PASSI	
3.4.1-A	Besoins opérationnels en matière de sécurité validés	• Définition des exigences liées au système • Matrice de traçabilité des exigences
3.4.2-A	Contrôles de sécurité de système	
3.4.4-A	Contrôles de sécurité de système approuvés	
3.5.1-B	Contrôles de sécurité de système révisés	
3.6.1-B	Version définitive des contrôles de sécurité de système	
3.4.3-A	Énoncé d'évaluation de l'adaptation des contrôles de sécurité	Rapport d'examen des bornes de l'analyse des besoins
3.5.1-A	Spécifications de la conception de système de haut niveau, incluant les contrôles de sécurité	Spécifications de la conception de système de haut niveau
3.5.3-A	Spécifications de la conception de système de haut niveau approuvées, incluant les contrôles de sécurité	
3.5.1-C	Résultats des activités d'EMR (de la phase de conception de haut niveau)	• Spécifications de la conception de système de haut niveau • Rapport d'EMR (au besoin)
3.5.2-A	Énoncé d'évaluation de la conception de système de haut niveau	Rapport d'examen des bornes de la conception de haut niveau
3.6.1-A	Spécifications de la conception de système détaillée, incluant les mécanismes de sécurité	Spécifications de la conception de système détaillée

N° d'identification	Extrants du PASSI	Produits livrables de projet de TI proposés
3.6.3-A	Spécifications approuvées de la conception de système détaillée, incluant les mécanismes de sécurité	
3.6.1-D	Résultats des activités d'EMR (de la phase de conception détaillée)	• Spécifications de la conception de système détaillée • Rapport d'EMR (au besoin)
3.6.2-A	Énoncé d'évaluation de la conception de système détaillée	Rapport d'examen des bornes de la conception détaillée
3.6.3-B	Autorisation de commencer la phase de développement	
3.7.1-A	Environnement de développement sécurisé	Sans objet
3.7.1-B	Documentation de l'environnement de développement	Documentation de l'environnement de développement
3.7.3-A	Représentation de la mise en œuvre du système d'information, incluant la sécurité	Représentation de la mise en œuvre du système d'information
3.7.3-B	Plans, scénarios et résultats des tests de la sécurité du développement	Documentation des tests de système
3.8.2-A	Plans, scénarios et résultats des tests d'intégration de la sécurité	
3.7.3-C	Procédures de sécurité opérationnelles	Procédures opérationnelles
3.7.3-D	Procédures d'installation des composants de sécurité	Procédures d'installation du système
3.7.2-A	Énoncé d'évaluation de l'environnement de développement sécurisé	Rapport d'examen des bornes du développement du système
3.7.4-A	Énoncé d'évaluation du développement de la sécurité	
3.8.1-A	Environnement de test du système d'information, incluant la sécurité	Sans objet
3.8.3-A	Énoncé d'évaluation des tests d'intégration de la sécurité	Rapport d'examen des bornes des tests du système
3.8.4-A	Autorisation de commencer la phase d'installation en production	
3.9.1-A	Environnement de production du système d'information, incluant la sécurité	Sans objet
3.9.1-B	Résultats de la vérification de l'installation des composants de sécurité	Rapport d'examen définitif de l'assurance de la qualité
3.9.3-A	Résultats de l'évaluation des risques résiduels	• Rapport d'évaluation des risques résiduels • Rapport d'EMR (au besoin)
3.9.4-A	Dispositions relatives à la sécurité du plan d'exploitation	Plan d'exploitation

N° d'identification	Extrants du PASSI	Produits livrables de projet de TI proposés
3.9.5-A	Trousse d'autorisation	Trousse d'autorisation
3.9.2-A	Énoncé d'évaluation de la vérification de l'installation des composants de sécurité	Rapport définitif d'examen des bornes
3.9.6-A	Autorisation de passer à l'étape d'exploitation	

Tableau 3 : Attribution proposée d'activités du PASSI aux rôles

Sous-sections	Activités du PASSI	Rôles (P = rôle principal, S = rôle de soutien)													
		Autorisateur	Gestionnaire de projet	Analyste opérationnel	Architecte de la sécurité (du ministère)	Concepteur de systèmes	Développeur de systèmes	Agent de sécurité du ministère	Intégrateur de systèmes	Testeur de systèmes	Coord. de la sécurité des TI	Praticien de la sécurité	Évaluateur de la sécurité (externe)	Administrateur de système	Personnel des opér. des TI
3.1	**Phase de motivation des intervenants**														
3.1.1	Identifier et motiver les intervenants de la sécurité	**S**	**P**												
3.2	**Phase de concept**														
3.2.1	Sélectionner les profils de contrôle de sécurité de domaine et les rapports d'évaluation des menaces applicables	**S**	**S**	**S**								**P**			
3.2.2	Déterminer la catégorie de sécurité du système d'information			**S**								**P**			
3.2.3	Cerner les exigences initiales d'assurance de la sécurité											**P**			
3.2.4	Approuver les exigences initiales d'assurance de la sécurité	**P**	**S**		**S**							**S**			
3.3	**Phase de planification**														
3.3.1	Intégrer les activités du PASSI au plan de projet		**P**									**S**			
3.3.2	Approuver le plan de projet	**P**	**S**					**S**			**S**				
3.4	**Phase d'analyse des besoins**														
3.4.1	Définir les besoins opérationnels en matière de sécurité			**S**	**S**							**P**			

Sous-sections	Activités du PASSI	Rôles (P = rôle principal, S = rôle de soutien)													
		Autorisateur	Gestionnaire de projet	Analyste opérationnel	Architecte de la sécurité (du ministère)	Concepteur de systèmes	Développeur de systèmes	Agent de sécurité du ministère	Intégrateur de systèmes	Testeur de systèmes	Coord. de la sécurité des TI	Praticien de la sécurité	Évaluateur de la sécurité (externe)	Administrateur de système	Personnel des opér. des TI
3.4.2	Adapter les contrôles de sécurité											P			
3.4.3	Évaluer l'adaptation des contrôles de sécurité											S	P		
3.4.4	Approuver les contrôles de sécurité de système	P											S		
3.5	**Phase de conception de haut niveau**														
3.5.1	Intégrer les contrôles de sécurité de système à la conception de haut niveau (appuyées par les activités d'EMR)					P			S			S			
3.5.2	Évaluer la conception de haut niveau											S	P		
3.5.3	Approuver la conception de haut niveau	P											S		
3.6	**Phase de conception détaillée**														
3.6.1	Intégrer les mécanismes de sécurité à la conception détaillée (appuyées par les activités d'EMR)					P			S			S			
3.6.2	Évaluer la conception détaillée											S	P		
3.6.3	Approuver la conception détaillée et le développement	P											S		
3.7	**Phase de développement**														
3.7.1	Établir un environnement de développement sécurisé						P					S			
3.7.2	Évaluer l'environnement de développement sécurisé											S	P		
3.7.3	Préciser, développer et tester les solutions de sécurité						P		S	S		S			
3.7.4	Évaluer le développement des solutions de sécurité											S	P		
3.8	**Phase d'intégration et de test**														
3.8.1	Installer des composants de sécurité dans l'environnement de test du								P			S			

Sous-sections	Activités du PASSI	Rôles (P = rôle principal, S = rôle de soutien)													
		Autorisateur	Gestionnaire de projet	Analyste opérationnel	Architecte de la sécurité (du ministère)	Concepteur de systèmes	Développeur de systèmes	Agent de sécurité du ministère	Intégrateur de systèmes	Testeur de systèmes	Coord. de la sécurité des TI	Praticien de la sécurité	Évaluateur de la sécurité (externe)	Administrateur de système	Personnel des opér. des TI
	système d'information														
3.8.2	Effectuer les tests d'intégration de la sécurité								S	P		S			
3.8.3	Évaluer les tests d'intégration de la sécurité											S	P		
3.8.4	Approuver l'installation en production	P											S		
3.9	**Phase d'installation**														
3.9.1	Installer et vérifier les composants de sécurité du système d'information dans l'environnement de production											S		P	
3.9.2	Évaluer la vérification de l'installation des composants de sécurité											S	P	S	
3.9.3	Effectuer une évaluation des risques résiduels											S	P		
3.9.4	Préparer les dispositions relatives à la sécurité du plan d'exploitation											P	S		S
3.9.5	Assembler la trousse d'autorisation											P	S		
3.9.6	Autoriser l'exploitation du système d'information	P	S										S		

3.1 Phase de motivation des intervenants

Cette sous-section décrit les activités du PASSI de la phase de motivation des intervenants du CDS, qui font partie de la phase de lancement du CVS.

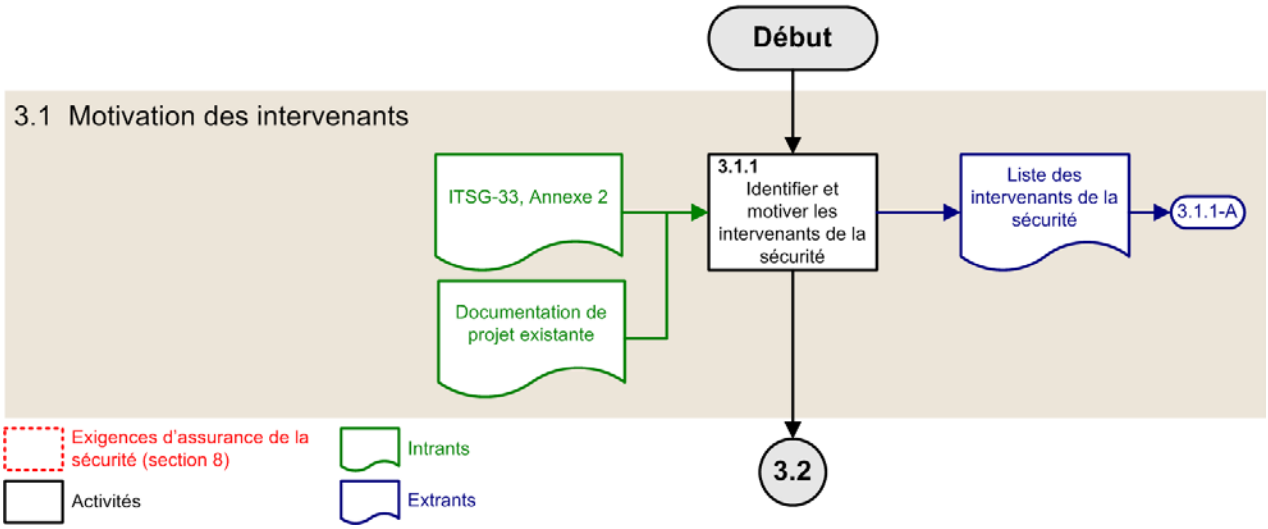


Figure 2 : Activités du PASSI – Phase de motivation des intervenants

3.1.1 Identifier et motiver les intervenants de la sécurité

Objectifs :	Identifier et motiver les intervenants de la sécurité du projet de TI.
Rôle principal :	Gestionnaire de projet
Rôles de soutien :	Autorisateur
Intrants :	ITSG-33, Annexe 2 – *Activités de gestion des risques liés à la sécurité des systèmes d'information* [le présent document] Documentation de projet existante
Extrants :	(3.1.1-A) Liste des intervenants de la sécurité
Exigences relatives à l'assurance de la sécurité :	Aucune exigence particulière

Lignes directrices :

Le PASSI mise sur la participation des cadres supérieurs du ministère pour obtenir les ressources et le financement appropriés au début du processus, pour examiner et approuver les extrants clés durant le

processus et pour autoriser l'exploitation du système d'information à la fin du processus. Le PASSI intervient donc au début de la phase de lancement du projet de TI pour veiller à ce que les intervenants de la sécurité soient identifiés et sensibilisés le plus tôt possible aux exigences du processus.

L'intervenant clé en matière de sécurité est le gestionnaire de la prestation de programmes et services, qui devra s'appuyer sur le système d'information pour s'acquitter de ses responsabilités. Le gestionnaire peut être l'autorisateur[4] (qui peut également être un employé de rang supérieur dans la structure hiérarchique, voir l'Annexe 1 du guide ITSG-33, section 5.13 [Référence 1]). Le rôle de l'autorisateur est d'autoriser l'utilisation du système d'information pour soutenir les objectifs de l'organisation. À ce titre, il assume la responsabilité de cette utilisation et en accepte donc les risques inhérents.

Un autre intervenant important est l'architecte de la sécurité ministérielle, dont le rôle consiste à développer les architectures et les normes de sécurité et à promulguer leur adoption au sein de l'organisation. Certains ministères possèdent leur propre architecte. Cette fonction peut également relever d'un cadre supérieur, p. ex., un dirigeant principal de l'information, un directeur des techniques informatiques ou une unité organisationnelle.

En plus de l'autorisateur et de l'architecte, les responsables des projets de TI peuvent exiger qu'un évaluateur externe de la sécurité, telle une autorité de certification, participe aux activités du PASSI. Certains ministères ont demandé à une autorité de certification de contribuer à l'évaluation des activités de sécurité. Dans ce cas particulier, les responsables du projet de TI doivent obtenir la participation de l'autorité à cette phase et déterminer exactement les activités d'évaluation de la sécurité qu'elle entend mener. Finalement, les responsables ont besoin du soutien de l'autorité opérationnelle des TI pour s'assurer de l'intégration appropriée du système d'information aux opérations de TI ministérielles existantes.

[4] L'autorisateur est parfois désigné sous le nom d'*autorité d'accréditation* dans le contexte d'un projet de TI.

3.2 Phase de concept

Cette sous-section décrit les activités du PASSI de la phase de concept du CDS, qui font partie de la phase de lancement du CVS.

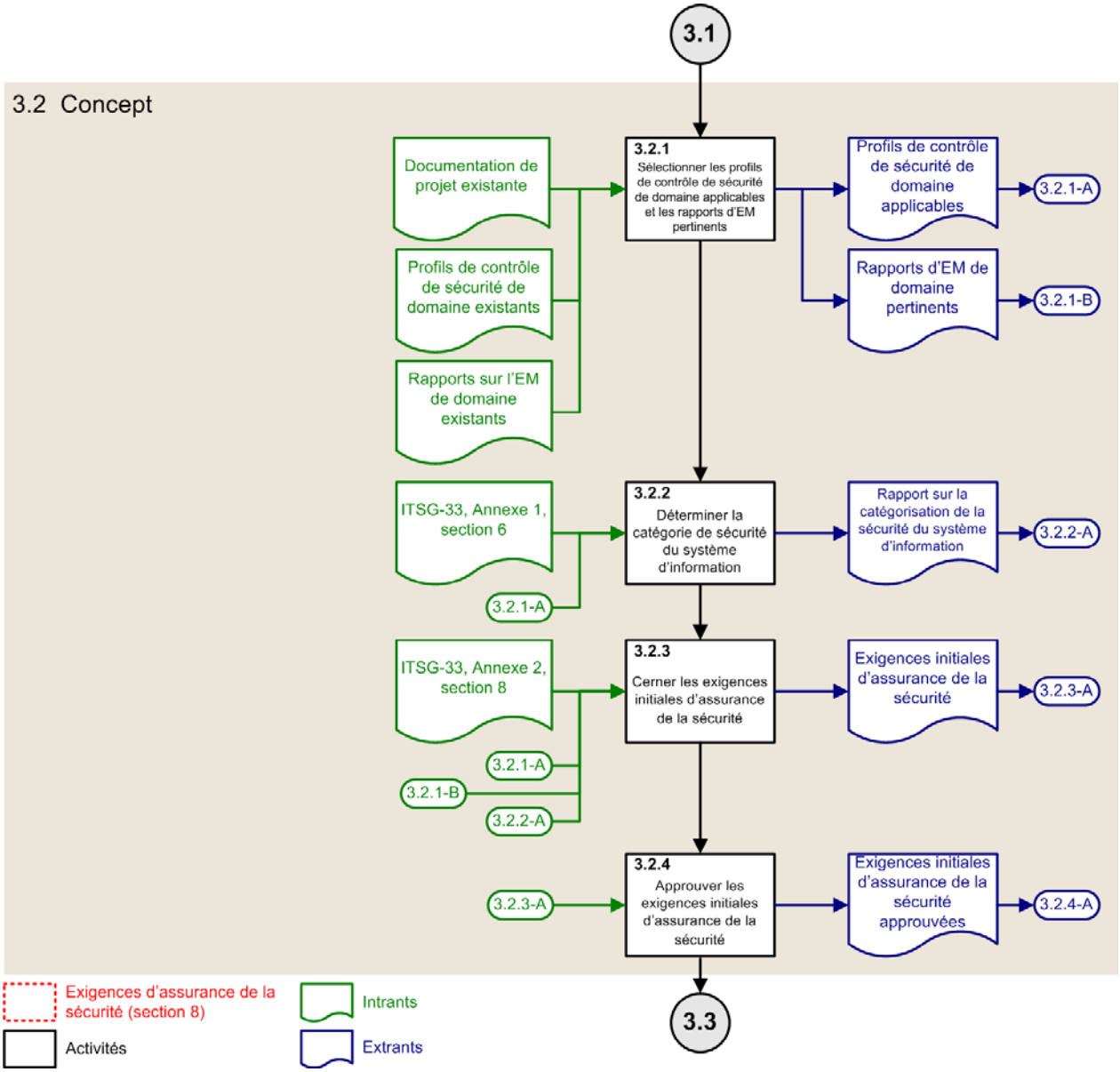


Figure 3 : Activités du PASSI – Phase de concept

Très tôt dans le processus de mise en œuvre, les responsables de projets de TI sélectionnent des profils de contrôle de sécurité de domaine (ou un profil de contrôle de sécurité ministériel, s'il n'existe aucun profil de domaine) qui s'appliquent aux activités opérationnelles que le système d'information prend en charge, et déterminent une catégorie de sécurité appropriée pour le système d'information. Les résultats de ces activités clés permettent la spécification d'un ensemble initial d'exigences d'assurance de la sécurité qui tient compte de la sensibilité et de la criticité des activités opérationnelles et de l'importance des menaces que ces dernières doivent contrer. Cet ensemble permet aux autorités du projet de TI de planifier adéquatement les aspects liés à la sécurité des TI de leur projet.

3.2.1 Sélectionner les profils de contrôle de sécurité de domaine applicables et les rapports d'évaluation des menaces pertinents

Objectifs :	Sélectionner les profils de contrôle de sécurité de domaine (ou les profils ministériels, s'il n'existe aucun profil de domaine) qui s'appliquent aux activités opérationnelles prises en charge par le système d'information, et les rapports d'évaluation des menaces qui concernent ces domaines et ces profils.
Rôle principal :	Praticien de la sécurité
Rôles de soutien :	Analyste opérationnel, autorisateur, gestionnaire de projet de TI
Intrants :	Documentation de projet existante Profils de contrôle de sécurité de domaine existants Rapports d'évaluation des menaces de domaine existants
Extrants :	(3.2.1-A) Profils de contrôle de sécurité de domaine applicables (3.2.1-B) Rapports d'évaluation des menaces de domaine pertinents
Exigences relatives à l'assurance de la sécurité :	Aucune exigence particulière

Lignes directrices :

Les profils de contrôle de sécurité de domaine prescrivent la mise en œuvre d'un ensemble de contrôles pour protéger des activités opérationnelles particulières contre certaines menaces. Il est donc important pour les praticiens de la sécurité de sélectionner les bons profils de domaine et les rapports d'évaluation des menaces pertinents afin d'établir une base appropriée pour l'adaptation et la mise en œuvre des contrôles de sécurité de leur système d'information. Le regroupement de contrôles applicables est effectué au cours du processus d'adaptation des contrôles (tel qu'il est décrit à la section 3.4.2).

Selon la nature de leurs programmes et services, les ministères peuvent utiliser un seul profil de contrôle de sécurité ministériel ou plusieurs profils de domaine. On utilise le terme profil de contrôle de sécurité de domaine dans le présent document.

Les autorités de la sécurité ministérielle ou l'autorisateur peuvent exiger l'utilisation d'un ou de plusieurs profils spécifiques de contrôle de sécurité de domaine pour le projet de TI. Sinon, les praticiens de la

sécurité devront soit sélectionner les profils applicables parmi les profils disponibles, soit en développer un spécifiquement pour les activités opérationnelles que leur système d'information prendra en charge s'il n'existe aucun profil applicable ou disponible. Les lignes directrices sur le développement des profils de contrôle de sécurité de domaine figurent à l'Annexe 1 du guide ITSG-33 [Référence 1].

Que les profils soient imposés ou sélectionnés, les praticiens de la sécurité doivent valider leur applicabilité aux activités opérationnelles que le système d'information prend en charge, ainsi que le contexte technique et de menace du projet.

Lorsqu'un seul profil de domaine est sélectionné pour un projet de TI, il faut toujours valider les hypothèses opérationnelles, techniques et de menace documentées dans le profil pour s'assurer qu'elles s'appliquent au contexte du projet.

Nota : Pour simplifier la teneur du texte dans le reste de la publication, nous nous en tiendrons à l'utilisation d'un seul profil applicable de contrôle de sécurité de domaine par projet de TI.

Lorsqu'ils sélectionnent des profils de contrôle, les praticiens exécutent les tâches suivantes :

- Validation du champ d'application du contexte opérationnel;
- Validation du champ d'application du contexte technique;
- Validation du champ d'application du contexte de menace;
- Validation du champ d'application des approches de sécurité de TI.

3.2.1.1 Valider le champ d'application du contexte opérationnel

Au tout début du projet de TI, il est utile que les praticiens de la sécurité comprennent le contexte du projet et les activités opérationnelles que le système d'information prend en charge et qu'ils valident cette information dans le contexte opérationnel du profil de domaine sélectionné. Plusieurs produits livrables de projet de TI, malgré qu'ils soient hors de la portée du PASSI, peuvent être utiles pour effectuer cette validation.

Par exemple, la charte de projet est une bonne source d'information et peut aider les praticiens à valider le contexte opérationnel puisqu'elle indique normalement les composants essentiels d'un projet, en particulier son objet, ses buts, sa portée, ses objectifs opérationnels, ses risques et ses hypothèses.

Les praticiens peuvent également tirer avantage de la documentation de projet qui définit les exigences qui sont propres au projet (p. ex., opérations, lois, protection des renseignements personnels, etc.).

L'exemple suivant permet d'illustrer le processus de validation du contexte opérationnel.

> Un praticien de la sécurité envisage d'utiliser un profil de contrôle de sécurité de domaine développé pour un contexte opérationnel où on mène des d'activités financières qui touchent de l'information cotée Protégé B. L'objectif du projet est d'ajouter une interface utilisateur à un système existant qui traite également de l'information cotée Protégé B. Puisque le système d'information du projet prendra en charge des activités opérationnelles qui s'inscrivent dans la portée du contexte opérationnel du profil en question, le praticien conclut que le contexte opérationnel de ce profil est applicable.

3.2.1.2 Valider le champ d'application du contexte technique

La deuxième étape du processus de validation d'un profil de contrôle de sécurité de domaine consiste à confirmer que le contexte technique et les hypothèses cernés dans le profil s'appliquent au contexte technique du projet de TI.

> Dans l'exemple de la section précédente, le praticien de la sécurité a déterminé que le contexte technique du profil est applicable aux systèmes financiers utilisés par quelques employés qui travaillent dans le même immeuble. L'objectif technique de son projet est d'étendre l'accès du système à un grand nombre d'employés répartis à l'échelle du pays et à certains partenaires privilégiés du domaine bancaire. Puisque le profil qu'il envisage d'utiliser a été développé pour un contexte technique différent, le praticien conclut qu'il devra l'adapter à ses besoins.

3.2.1.3 Valider le champ d'application du contexte de menace

La troisième étape du processus de validation consiste à confirmer que les menaces cernées dans la section du contexte de menace du profil (définies plus en détail dans le rapport d'évaluation des menaces de domaine associé au profil, le cas échéant) s'appliquent aux activités opérationnelles que le système d'information prend en charge.

> Pour continuer avec l'exemple de la section 3.2.1.1, le praticien détermine que le profil envisagé a été développé pour contrer des menaces peu complexes étant donné que le contexte technique présumait que les systèmes d'information de soutien ne seraient pas connectés directement à des réseaux externes et que les activités opérationnelles de domaine ne seraient donc pas exposées à des attaques externes sophistiquées. Un des objectifs techniques de son projet est de relier le système financier existant à un site dans un pays étranger pour un événement spécial ponctuel. Comme le profil envisagé a été développé pour un contexte de menace différent, le praticien conclut donc qu'il lui faudra déployer des efforts d'adaptation importants pour qu'il réponde à ses besoins.

3.2.1.4 Valider le champ d'application des approches de sécurité de TI

La quatrième étape du processus de validation consiste à confirmer que les approches de sécurité de TI documentées dans le profil sont compatibles avec les objectifs du projet de TI.

> Toujours dans le contexte de l'exemple de la section 3.2.1.1, le praticien détermine que les approches de sécurité de TI du profil envisagé incluent l'établissement d'un périmètre de réseau solide autour des composants du système d'information afin de réduire les besoins de contrôles de sécurité internes et, du fait même, la complexité et les coûts de la solution. Un des objectifs de son projet est de relier un grand nombre de clients au système financier par une nouvelle interface centralisée et de bénéficier ainsi d'une approche de périmètre de réseau solide. Puisque le projet appliquera des approches de sécurité des TI qui s'inscrivent dans la portée des approches du profil envisagé, le praticien conclut que ces approches sont applicables.

3.2.2 Déterminer la catégorie de sécurité du système d'information

Objectifs :	Déterminer la catégorie de sécurité du système d'information en fonction des activités opérationnelles (c.-à-d., processus opérationnels et information connexe) qu'il prendra en charge.
Rôle principal :	Praticien de la sécurité
Rôles de soutien :	Analyste opérationnel
Intrants :	ITSG-33, Annexe 1, section 6 – *Processus de catégorisation de la sécurité* [Référence 1] (3.2.1-A) Profils de contrôle de sécurité de domaine applicables
Extrants :	(3.2.2-A) Rapport sur la catégorisation de la sécurité du système d'information
Exigences relatives à l'assurance de la sécurité :	Aucune exigence particulière

Lignes directrices :

Dans l'activité précédente (section 3.2.1), nous avons confirmé que les profils de contrôle de sécurité de domaine sont applicables au projet de TI. Ces profils ont été développés pour être appliqués à des types d'activités opérationnelles spécifiques (incluant les ressources d'information connexes). La catégorie de sécurité de ces activités[5] est documentée dans les profils et habituellement incluse dans le nom du profil (p. ex., *Profil pour les activités liées aux rapports administratifs – Catégorie de sécurité cotée Protégé A, intégrité et disponibilité faibles*).

Dans cette activité, les responsables du projet doivent préciser une catégorie de sécurité pour le système d'information qui sera mis en œuvre. Cette catégorie indique que le système est mis en place et exploité pour répondre aux objectifs de sécurité.

On recommande qu'un système d'information hérite de la catégorie de sécurité des activités opérationnelles qu'il prend en charge, tel que documenté dans les profils validés. Cela signifie simplement que le système est mis en place et exploité pour répondre aux besoins de sécurité des activités opérationnelles.

Dans le cas d'un profil individuel déclaré applicable, la catégorie de sécurité du système d'information doit être identique à celle des activités opérationnelles documentées dans le profil. Lorsque plusieurs profils de contrôle de sécurité de domaine s'appliquent, on recommande que la catégorie de sécurité du système d'information corresponde à la catégorie la plus élevée de tous les profils (c.-à-d., catégorie maximale) afin que le système soit en mesure de satisfaire à tous les objectifs de sécurité de toutes les activités opérationnelles prises en charge.

[5] Comme il est décrit à l'Annexe 1 du guide ITSG-33 [Référence 1], la catégorie de sécurité d'une activité opérationnelle est établie en déterminant le niveau de préjudice auquel on peut raisonnablement s'attendre dans l'éventualité d'une compromission de la confidentialité, de l'intégrité et de la disponibilité des biens de TI connexes. Par exemple, si l'on s'attend que la compromission de la disponibilité d'un système d'information, utilisé pour offrir des services aux citoyens, entraîne des préjudices moyens à leur égard, on attribue à la disponibilité de l'activité une catégorie de sécurité moyenne. La même logique est appliquée à la confidentialité et à l'intégrité.

Par exemple :

Activité opérationnelle	**Catégorie de sécurité de l'activité opérationnelle**		
	Confidentialité	**Intégrité**	**Disponibilité**
Analyse de données de capteur	Non classifié	**Moyenne**	Faible
Rapports administratifs	**Protégé A**	Faible	Faible
Catégorie du système d'information	**Protégé A**	**Moyenne**	**Faible**

Si les responsables du projet décident de sélectionner une catégorie de sécurité différente pour le système d'information en utilisant une méthode différente de celle suggérée ci-dessus (p. ex., pour la réduction des coûts), l'autorisateur doit approuver la décision et accepter les risques.

Voir l'Annexe 1 du guide ITSG-33 [Référence 1] pour plus de détails sur les profils de contrôle de sécurité de domaine et la catégorisation de sécurité des activités opérationnelles.

3.2.3 Cerner les exigences initiales d'assurance de la sécurité

Objectifs :	Cerner les exigences initiales d'assurance de la sécurité prescrites pour le système d'information.
Rôle principal :	Praticien de la sécurité
Rôles de soutien :	Aucun
Intrants :	ITSG-33, Annexe 2, section 8 – *Exigences d'assurance de la sécurité* [le présent document] (3.2.1-A) Profils de contrôle de sécurité de domaine applicables (3.2.1-B) Rapports d'évaluation des menaces de domaine pertinents (3.2.2-A) Rapport sur la catégorisation de la sécurité du système d'information
Extrants :	(3.2.3-A) Exigences initiales d'assurance de la sécurité
Exigences relatives à l'assurance de la sécurité :	Aucune exigence particulière

Lignes directrices :

Les exigences d'assurance de la sécurité précisent les tâches liées à la sécurité qui doivent être exécutées dans le cadre des projets de TI tout au long du PASSI pour accroître la confiance envers la pertinence des mécanismes de sécurité mis en place. De manière générale, chaque exigence inclut des tâches techniques (c.-à-d. travaux techniques et documentation à produire), des exigences relatives au contenu des documents

(c.-à-d. contenu et preuves à inclure dans les résultats des tâches techniques) et des tâches d'évaluation (c.-à-d. travail nécessaire pour évaluer les tâches techniques et leurs résultats).

Les lignes directrices de la présente annexe indiquent à quel moment dans les activités du PASSI les exigences d'assurance de la sécurité entrent en jeu. Les exigences d'assurance de la sécurité (tâches techniques, exigences relatives au contenu des documents et tâches d'évaluation) sont définies à la section 8.

Dans des circonstances normales, le profil de contrôle de sécurité applicable précise les exigences qui peuvent composer l'ensemble initial d'exigences pour le projet. Sinon, les praticiens de la sécurité peuvent suivre le processus suivant :

1) La catégorie de sécurité du système d'information, documentée dans le rapport sur la catégorisation de sécurité du système d'information (section 3.2.2), permet de déterminer le niveau de préjudice le plus élevé des objectifs de confidentialité, d'intégrité et de disponibilité. Par exemple, si la catégorie de sécurité du système d'information est cotée Protégé B, avec une intégrité moyenne et une disponibilité élevée, le niveau de préjudice le plus élevé est le niveau élevé. Si la catégorie de sécurité est cotée Protégé B, avec une intégrité faible et une disponibilité faible, le niveau de préjudice le plus élevé est le niveau moyen;

2) Le processus décrit à la section 7.4.2 et l'information sur les menaces contenue dans le profil de contrôle de sécurité de domaine applicable et le rapport d'évaluation des menaces de domaine (le cas échéant) ou le rapport ministériel d'évaluation des menaces permettent de déterminer la catégorie la plus élevée de capacités des agents de menace (menaces délibérées) et l'ampleur des événements (menaces accidentelles et risques naturels);

3) Le Tableau 7 et les lignes directrices à la section 7.4.3, utilisés comme guide, permettent de déterminer le niveau de robustesse correspondant au niveau de préjudice le plus élevé déterminé à l'étape 1 et aux catégories de menace les plus élevées déterminées à l'étape 2. Le niveau correspondant représente le niveau maximal global de robustesse[6] du système. Ce niveau concerne l'ensemble du système (boîte noire) et représente normalement le niveau requis pour la mise en œuvre des contrôles de sécurité critiques. Cela ne signifie pas, toutefois, que tous les contrôles de sécurité de système seront appliqués à ce niveau. La détermination du niveau de robustesse propre aux contrôles de sécurité est effectuée durant les phases d'analyse de la conception;

4) Le Tableau 4 à la section 7.3 permet de déterminer niveau d'assurance de la sécurité (NAS) correspondant au niveau de robustesse initial;

5) Le Tableau 9 à la section 8.3 permet de déterminer l'ensemble initial des exigences d'assurance de la sécurité.

Notons que ce processus permet d'obtenir le niveau d'assurance de la sécurité le plus strict requis pour le projet. Ce niveau sera ajusté au cours des phases de conception pour assurer un juste équilibre entre l'assurance de la sécurité et la rentabilité du projet. Il faut avoir une certaine connaissance des exigences d'assurance de la sécurité à ce stade préliminaire pour faciliter la planification du projet. Ces exigences seront ajustées ultérieurement, durant les phases de conception, pour tenir compte des exigences de robustesse plus spécifiques propres aux contrôles de sécurité.

[6] Voir la section 7 pour plus de détails sur la robustesse.

3.2.4 Approuver les exigences initiales d'assurance de la sécurité

Objectifs :	Obtenir l'autorisation de commencer la phase de planification du projet en tenant compte des exigences initiales d'assurance de la sécurité.
Rôle principal :	Autorisateur
Rôles de soutien :	Architecte fonctionnel ou de la sécurité ministérielle, gestionnaire de projet, praticien de la sécurité
Intrants :	(3.2.3-A) Exigences initiales d'assurance de la sécurité
Extrants :	(3.2.4-A) Exigences initiales d'assurance de la sécurité approuvées
Exigences relatives à l'assurance de la sécurité :	Aucune exigence particulière

Lignes directrices :

Avant d'entreprendre la phase de planification, les responsables de projets de TI doivent examiner avec l'autorisateur les extrants du PASSI de la phase de concept et obtenir son approbation des exigences initiales d'assurance de la sécurité. Les extrants de la phase de concept établissent le niveau d'effort requis pour les activités d'ingénierie et d'évaluation de la sécurité de l'ensemble du projet et constituent donc des facteurs importants pour déterminer les coûts et le calendrier du projet.

Les responsables des projets doivent planifier cette activité en même temps que les activités d'établissement des bornes de la phase de concept de leur CDS.

Au cours de l'examen des extrants du PASSI de la phase de concept, les autorisateurs doivent tenir compte de ce qui suit :

- Examiner, avec les agents de sécurité du ministère et un architecte fonctionnel ou de la sécurité ministérielle (si ce poste existe au sein du ministère), les approches de sécurité définies dans le profil de contrôle de sécurité de domaine applicable pour comprendre leur incidence sur la complexité du projet et sur les exigences en matière de connaissances, de compétences et d'expérience des membres de l'équipe;
- Examiner avec le praticien de la sécurité la catégorie de sécurité sélectionnée pour le système d'information afin de s'assurer que les activités opérationnelles ont été correctement cernées et que des niveaux de catégorie de sécurité appropriés ont été sélectionnés pour les objectifs de confidentialité, d'intégrité et de disponibilité du système d'information;
- Examiner, avec le gestionnaire de projet et le praticien de la sécurité, les exigences initiales d'assurance de la sécurité sélectionnées pour comprendre leur incidence sur les coûts, les ressources et le calendrier du projet.

3.3 Phase de planification

Cette sous-section décrit les activités du PASSI de la phase de planification du CDS, qui font partie de la phase de lancement du CVS.

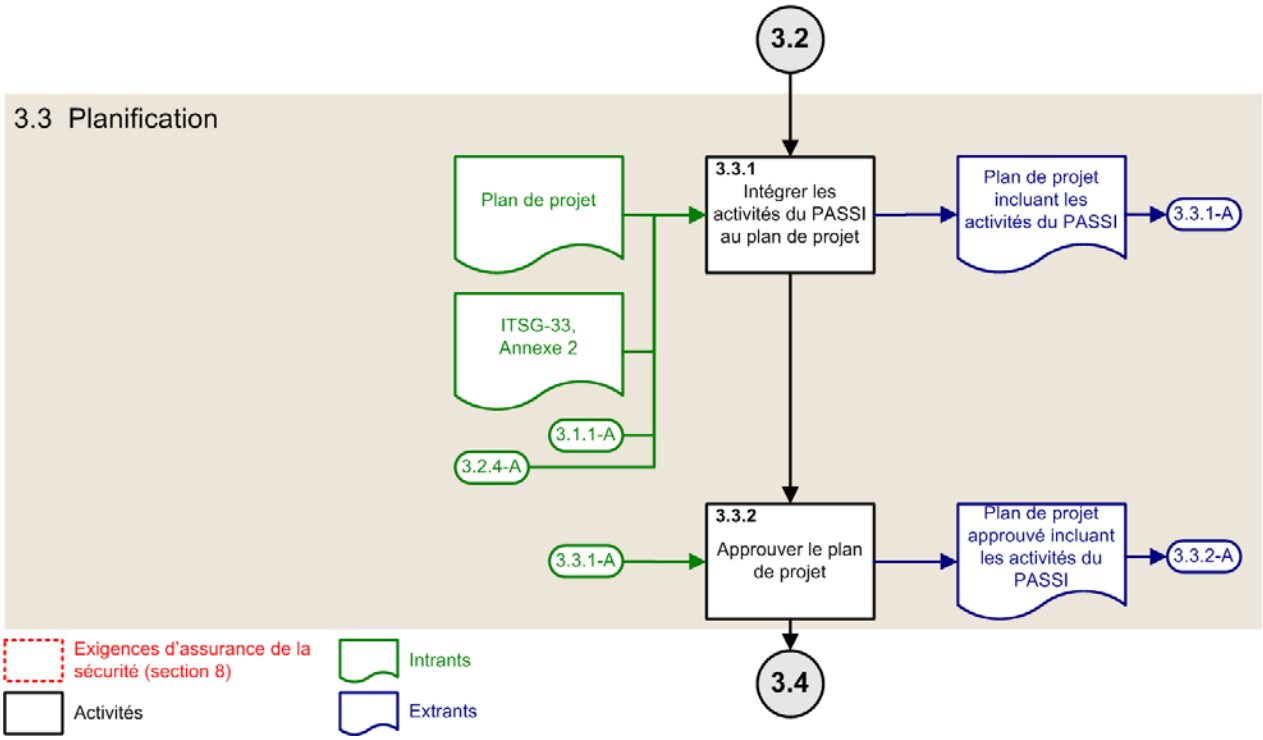


Figure 4 : Activités du PASSI – Phase de planification

3.3.1 Intégrer les activités du PASSI au plan de projet

Objectifs :	Planifier les aspects liés à la sécurité du projet.
Rôle principal :	Gestionnaire de projet
Rôles de soutien :	Praticien de la sécurité
Intrants :	Plan de projet ITSG-33, Annexe 2 – *Activités de gestion des risques liés à la sécurité des systèmes d'information* [le présent document] (3.1.1-A) Liste des intervenants de la sécurité (qui détermine, en partie, l'attribution des tâches du projet) (3.2.4.-A) Exigences initiales d'assurance de la sécurité approuvées
Extrants :	(3.3.1-A) Plan de projet incluant les activités du PASSI
Exigences relatives à l'assurance de la sécurité :	Aucune exigence particulière

Lignes directrices :

Pour obtenir les meilleurs résultats, on doit intégrer les activités du PASSI au plan de projet plutôt que d'utiliser un plan distinct.

Dans un projet de TI type, le gestionnaire de projet, en collaboration avec les praticiens de la sécurité et avec la participation de l'autorisateur, adapte le PASSI pour tenir compte de l'objectif (p. ex., mise en œuvre d'un nouveau système ou modifications ou améliorations d'un système existant) et de la complexité du projet (p. ex., création d'un site Web, déploiement de l'infrastructure technique, création d'une application financière ou militaire personnalisée). Les responsables de projets de TI adaptent également le PASSI en fonction de la disponibilité des produits livrables associés aux processus ministériels (p. ex., profils de contrôle de sécurité de domaine). Dans le cas de projets pour lesquels il n'existe aucun profil de contrôle de sécurité de domaine applicable, les responsables doivent prévoir des activités supplémentaires pour en développer un. Dans ce cas, les autorités de projet doivent solliciter la participation du coordonnateur de la sécurité des TI de leur ministère et du secteur opérationnel concerné.

Les responsables des projets de TI doivent évaluer les coûts liés à la sécurité dans le cadre des activités d'établissement des coûts globaux pour assurer un financement suffisant du projet. Il y a plusieurs aspects liés à l'application de la sécurité dans les systèmes d'information dont on doit tenir compte au moment d'évaluer les coûts des projets de TI :

- Nature des activités opérationnelles prises en charge par le système d'information (p. ex., un simple site Web public par opposition à un poste de commande et de contrôle militaire) et catégorie de sécurité du système (p. ex., Protégé B par opposition à Classifié);
- Nature de l'environnement technique et type et complexité de la stratégie de sécurité globale définie dans les approches de sécurité décrites dans le profil de contrôle de sécurité de domaine applicable (p. ex., un système spécialisé autonome non connecté à des réseaux externes par

opposition à un système hautement distribué, qui offre des services à différents types de collectivité d'utilisateurs, et axé sur une sécurité d'application distribuée);

- Exigences d'assurance de la sécurité et leur incidence sur le niveau d'effort que requièrent l'ingénierie de sécurité, l'évaluation de la sécurité et la documentation du système, et sur l'établissement et la gestion de l'environnement de développement;
- Disponibilité d'un profil de contrôle de sécurité de domaine applicable et d'un rapport d'évaluation des menaces de domaine. Les responsables qui ne peuvent trouver ni ce profil, ni le rapport d'évaluation doivent se fier à un profil et à un rapport ministériels ou, dans certains cas, développer un profil de contrôle de sécurité de domaine, ce qui risque d'accroître le niveau d'effort nécessaire pour définir et adapter les contrôles de sécurité et mener les activités d'évaluation des menaces et des risques (EMR).

Il importe de noter que le sous-financement des activités de sécurité est susceptible de mener à la mise en œuvre de systèmes d'information moins sécurisés et de placer les autorisateurs dans une situation où ils doivent accepter de plus grands risques résiduels.

Consulter le Tableau 3 pour les recommandations concernant l'attribution des activités du PASSI aux différents rôles, et l'Annexe 1 du guide ITSG-33 [Référence 1] pour les lignes directrices sur les rôles et les responsabilités.

3.3.2 Approuver le plan de projet

Objectifs :	Obtenir l'autorisation de poursuivre le projet conformément au plan de projet.
Rôle principal :	Autorisateur
Rôles de soutien :	Gestionnaire de projet, agent de sécurité ministériel, coordonnateur de la sécurité des TI
Intrants :	(3.3.1-A) Plan de projet incluant les activités du PASSI
Extrants :	(3.3.2-A) Plan de projet approuvé incluant les activités du PASSI
Exigences relatives à l'assurance de la sécurité :	Aucune exigence particulière

Lignes directrices :

Le but principal de cette activité est d'obtenir de l'autorisateur l'approbation de poursuivre le projet de TI conformément au plan de projet. À partir de cette étape, tout changement apporté aux activités de sécurité prévues peut accroître les coûts du projet, influer sur le calendrier des tâches, réduire la confiance envers la posture de sécurité du système d'information et mener à des niveaux de risque résiduel plus élevés.

3.4 Phase d'analyse des besoins

Cette sous-section décrit les activités du PASSI de la phase d'analyse des besoins du CDS, qui font partie de la phase de lancement du CVS.

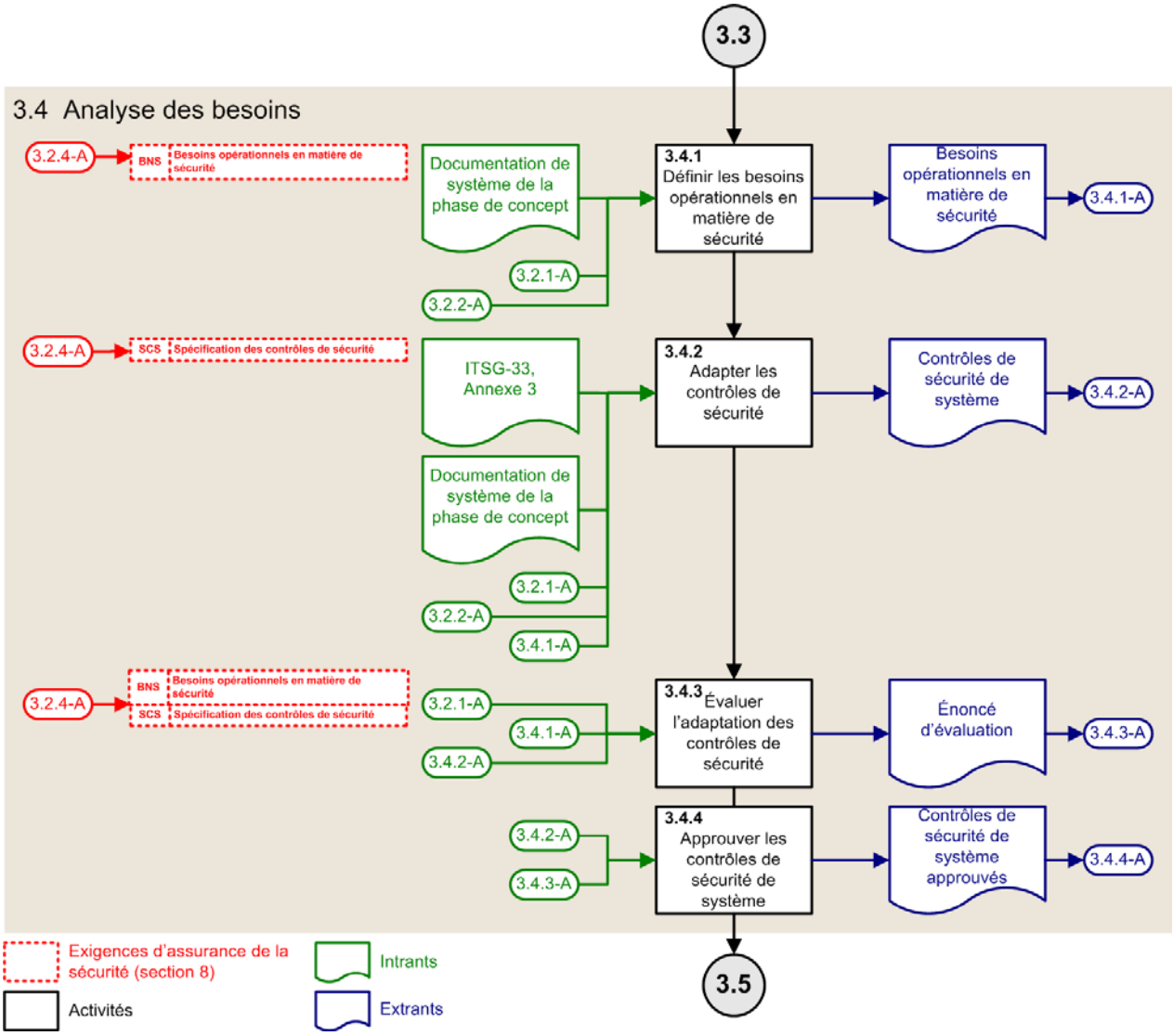


Figure 5 : Activités du PASSI – Phase d'analyse des besoins

3.4.1 Définir les besoins opérationnels en matière de sécurité

Objectifs :	Définir les besoins opérationnels en matière de sécurité auxquels le système d'information doit répondre.
Rôle principal :	Praticien de la sécurité
Rôles de soutien :	Analyste opérationnel, architecte fonctionnel ou de la sécurité ministérielle
Intrants :	Documentation du système de la phase de concept (p. ex., concept des opérations) (3.2.1-A) Profils de contrôle de sécurité de domaine applicables (3.2.2-A) Rapport sur la catégorisation de la sécurité du système d'information
Extrants :	(3.4.1-A) Besoins opérationnels en matière de sécurité
Exigences relatives à l'assurance de la sécurité :	(3.2.4.-A) Tâches techniques et exigences relatives au contenu des documents d'assurance de la sécurité pour les besoins opérationnels en matière de sécurité (section 8, BNS-E et BNS-D)

Lignes directrices :

Les besoins opérationnels en matière de sécurité répondent aux exigences de l'autorisateur, du responsable opérationnel et des autres intervenants en matière de sécurité. Ils définissent, en termes opérationnels, les besoins de protection des processus (et de l'information connexe) de chaque activité opérationnelle pour permettre l'atteinte des objectifs de sécurité sur le plan de la confidentialité, de l'intégrité et de la disponibilité. Ils sont dérivés des lois, des règlements, des politiques, des directives, des normes, des obligations contractuelles et des objectifs qui gouvernent les activités opérationnelles. Lorsqu'ils appuient les activités opérationnelles, les systèmes doivent répondre à leurs besoins en matière de confidentialité, d'intégrité et de disponibilité en appliquant les contrôles de sécurité de TI appropriés.

Ces besoins doivent être définis, en tout ou en partie, dans le profil de contrôle de sécurité de domaine applicable. Les praticiens examinent ensuite à ces besoins prédéfinis et les comparent à la documentation de projet pour confirmer la mesure dans laquelle ils s'appliquent au projet de TI et pour cerner et définir tout besoin supplémentaire non documenté dans le profil.

Les responsables des projets de TI doivent définir les besoins opérationnels avec l'aide d'un analyste opérationnel compétent. Ils doivent également s'assurer de la collaboration d'un architecte fonctionnel ou de la sécurité ministérielle (personne ou groupe, le cas échéant) qui doit connaître les besoins et être en mesure de combler les écarts entre les exigences et le système d'information qu'on prévoit éventuellement développer ou mettre à jour dans le cadre du projet de TI.

L'Annexe 1 du guide ITSG-33 [Référence 1] donne plus de détails sur les besoins opérationnels en matière de sécurité et les profils de contrôle de sécurité de domaine.

3.4.2 Adapter les contrôles de sécurité

Objectifs :	Adapter les contrôles de sécurité pour répondre aux exigences du système telles que définies par le profil de contrôle de sécurité de domaine applicable et par la catégorie de sécurité et les besoins opérationnels en matière de sécurité. Examiner les descriptions des contrôles de sécurité de système pour s'assurer qu'elles sont rédigées d'une manière non ambiguë et qu'elles fournissent de l'information claire aux concepteurs de systèmes et aux praticiens de la sécurité qui effectueront ultérieurement les travaux de conception, et vérifier que des exigences de sécurité précises sont incluses dans les demandes de proposition (DP) requises pour l'impartition de certains aspects des travaux de mise en œuvre.
Rôle principal :	Praticien de la sécurité
Rôles de soutien :	Aucun
Intrants :	ITSG-33, Annexe 3 – *Catalogue des contrôles de sécurité* [Référence 7] Documentation du système de la phase de concept (p. ex., concept des opérations) (3.2.1-A) Profils de contrôle de sécurité de domaine applicables (3.2.2-A) Rapport sur la catégorisation de la sécurité du système d'information (3.4.1-A) Besoins opérationnels en matière de sécurité
Extrants :	(3.4.2-A) Contrôles de sécurité de système
Exigences relatives à l'assurance de la sécurité :	(3.2.4-A) Tâches techniques d'assurance de la sécurité et exigences relatives au contenu de la documentation pour la spécification de contrôle de sécurité (section 8, SCS-E et SCS-D)

Lignes directrices :

Le principal intrant de cette activité est un profil de contrôle de sécurité de domaine. Ce profil documente l'ensemble des contrôles de sécurité applicables au projet de TI exigés par le ministère et définis à l'Annexe 3 du guide ITSG-33 [Référence 7]. Chaque contrôle inclut des exigences fonctionnelles de sécurité de base et autant d'améliorations que nécessaire pour augmenter la protection offerte par cette fonction de base.

Le processus d'adaptation des contrôles de sécurité peut être résumé comme suit :

1) Sélectionner dans le profil applicable les contrôles et les améliorations qui s'appliquent au système d'information. Comme il est décrit à l'Annexe 1 du guide ITSG-33 [Référence 1], le profil doit inclure des directives concernant les responsables les plus aptes à effectuer la mise en œuvre et à assurer le fonctionnement des contrôles;

2) Le cas échéant, adapter les contrôles et les améliorations pour répondre aux besoins opérationnels en matière de sécurité du système d'information;

3) Rationaliser les contrôles et les améliorations afin d'optimiser l'adaptation. Documenter la justification des ajouts et des suppressions de contrôles et d'améliorations pour l'évaluateur de la sécurité et l'autorisateur;

4) Améliorer les définitions des contrôles pour s'assurer qu'elles sont rédigées d'une manière non ambiguë et qu'elles fournissent de l'information claire aux praticiens de la sécurité qui effectueront ultérieurement les travaux de conception.

L'adaptation permet aux praticiens de préciser les paramètres de contrôle non définis, de sélectionner des contrôles et des améliorations supplémentaires et de supprimer ceux qui sont inutiles ou non applicables. Les praticiens doivent documenter leur justification pour tous les ajouts et toutes les suppressions afin d'en informer l'évaluateur et l'autorisateur.

Au moment d'adapter des contrôles à un système d'information particulier, les praticiens doivent examiner le profil de contrôle de sécurité de domaine applicable et les documents pertinents pour s'assurer qu'aucune exigence nouvelle ou supplémentaire n'a été ajoutée au profil. À cette fin, ils doivent tenir compte de ce qui suit :

- Politiques, normes et procédures organisationnelles relatives aux activités opérationnelles;
- Instruments réglementaires, exigences contractuelles et exigences de sécurité ministérielle applicables spécifiquement au projet de TI;
- Normes ministérielles relatives aux TI et à leur sécurité, telles celles définies dans les artefacts de l'architecture d'entreprise, qui peuvent contenir des exigences et des contraintes techniques;
- Environnement de menace défini dans le rapport d'évaluation des menaces de domaine.

Les praticiens peuvent également adapter les contrôles de sécurité à la lumière de l'information sur les risques vraisemblablement disponible à ce stade (p. ex., une menace importante ayant donné lieu récemment à la compromission d'un système d'information ministériel existant, une vulnérabilité connue qui affecte de la même manière tous les systèmes ministériels).

À ce stade-ci, le produit du processus d'adaptation est un ensemble de contrôles de sécurité de système qui feront l'objet d'une adaptation et d'une amélioration plus poussées durant les activités de soutien de l'EMR et le processus de conception de système et de la sécurité du PASSI.

3.4.2.1 Matrice de traçabilité des exigences de sécurité (MTES)

Une façon de s'assurer que les projets de TI répondent à plusieurs des exigences d'assurance de la sécurité est d'utiliser une matrice de traçabilité des exigences de sécurité ou MTES. La MTES est l'outil approprié lorsque les exigences demandent de tracer la correspondance entre les exigences du système d'information et les spécifications de conception.

Grâce à la MTES, les responsables du projet peuvent répondre à l'objectif de l'assurance et s'assurer que les spécifications de contrôle décrivent de manière bien définie et non ambiguë les contrôles de sécurité applicables.

Au cours du PASSI, les responsables des projets de TI peuvent utiliser la MTES aux fins suivantes :

- Durant le processus de validation des besoins opérationnels en matière de sécurité (section 3.4.1), documenter les besoins et les mettre en correspondance avec les objectifs ministériels visés (section 8.4.1);

- Durant le processus d'adaptation des contrôles de sécurité (section 3.4.2), documenter les contrôles de sécurité de système et les mettre en correspondance avec les besoins opérationnels et les autres exigences de haut niveau auxquelles ils répondent (section 8.4.2);
- Durant le processus de conception de haut niveau (section 3.5.1), mettre les spécifications de conception en correspondance avec leurs contrôles de sécurité de système (section 8.4.3), et mettre les contrôles de sécurité de système en correspondance avec les menaces qu'ils doivent contrer (section 8.4.4);
- Durant le processus de conception détaillée (section 3.6.1), mettre les mécanismes de sécurité en correspondance avec leurs contrôles de sécurité de système (section 8.4.3), et mettre les mécanismes de sécurité de système en correspondance avec les menaces qu'ils doivent contrer (section 8.4.4);
- Au cours du développement des scénarios de test durant le processus de développement du système d'information (section 3.7.3), mettre les scénarios en correspondance avec les mécanismes de sécurité (section 8.4.9).

La MTES peut être intégrée à la matrice plus large de traçabilité des exigences du projet, s'il y a lieu.

3.4.3 Évaluer l'adaptation des contrôles de sécurité

Objectifs :	Confirmer que le processus d'adaptation des contrôles de sécurité a été effectué en conformité avec les exigences d'assurance de la sécurité.
Rôle principal :	Évaluateur de la sécurité
Rôles de soutien :	Praticien de la sécurité
Intrants :	(3.2.1-A) Profils de contrôle de sécurité de domaine applicables (3.4.1-A) Besoins opérationnels en matière de sécurité (3.4.2-A) Contrôles de sécurité de système
Extrants :	(3.4.3-A) Énoncé d'évaluation de l'adaptation des contrôles de sécurité
Exigences relatives à l'assurance de la sécurité :	(3.2.4-A) Tâches d'évaluation d'assurance de la sécurité pour les besoins opérationnels en matière de sécurité et spécification de contrôle de sécurité (section 8, BNS-A et SCS-A)

Lignes directrices :

De pair avec le praticien de la sécurité, l'évaluateur de la sécurité doit effectuer les tâches suivantes :

- Confirmer que la définition des besoins opérationnels en matière de sécurité correspond aux tâches techniques et respecte les exigences relatives au contenu des documents;
- Confirmer que les travaux d'adaptation des contrôles correspondent aux tâches techniques et respectent les exigences relatives au contenu des documents;
- Préparer un énoncé d'évaluation aux fins d'approbation.

Le terme *énoncé d'évaluation* est utilisé pour désigner la reconnaissance ou la confirmation que le processus d'évaluation a été suivi et que ses résultats sont acceptables. L'énoncé peut être aussi simple qu'un compte rendu de décision d'un procès-verbal d'une réunion technique ou de projet, ou aussi formel qu'un certificat d'évaluation signé par un évaluateur de la sécurité.

Note importante concernant les activités d'évaluation et d'approbation :

Bien que l'on indique que les activités d'évaluation et d'approbation de la sécurité du PASSI sont menées à la fin de leur phase respective, en pratique, les évaluateurs de la sécurité doivent participer activement à leur conduite, examiner les extrants du processus au fur et à mesure de leur production et informer immédiatement les autorisateurs des problèmes de sécurité et de leur incidence sur les objectifs de sécurité et les risques connexes. Ainsi, les évaluateurs peuvent s'assurer que les responsables des projets de TI corrigent les problèmes au fur et à mesure qu'ils sont relevés en demandant que des corrections soient apportées aux produits du PASSI et que l'équipe de projet effectue des travaux supplémentaires (p. ex., refaire les tests de sécurité), ou toute autre activité corrective jugée pertinente, plutôt que d'attendre à la fin de la phase et risquer des retards, des coûts de projet supplémentaires et des risques inacceptables.

Toutefois, il peut arriver qu'un problème de sécurité particulier ne puisse être corrigé. Dans ce cas, les évaluateurs doivent immédiatement informer leur autorisateur, lui indiquer l'incidence potentielle du problème sur les objectifs de sécurité et les risques et obtenir l'autorisation de poursuivre le projet avec ou sans la mise en œuvre de mesures de compensation. Enfin, les évaluateurs doivent documenter les problèmes non réglés dans des énoncés d'évaluation et inclure une justification et les résultats de l'évaluation des risques.

3.4.4 Approuver les contrôles de sécurité de système

Objectifs :	Obtenir l'autorisation de commencer la conception de haut niveau du système d'information au moyen l'ensemble de contrôles de sécurité de système adaptés.
Rôle principal :	Autorisateur
Rôles de soutien :	Évaluateur de la sécurité
Intrants :	(3.4.2-A) Contrôles de sécurité de système (3.4.3-A) Énoncé d'évaluation de l'adaptation des contrôles de sécurité
Extrants :	(3.4.4-A) Contrôles de sécurité de système approuvés
Exigences relatives à l'assurance de la sécurité :	Aucune exigence particulière

Lignes directrices :

Le but principal de cette activité est d'obtenir de l'autorisateur qu'il approuve le lancement de la phase de conception de haut niveau du projet de TI au moyen des contrôles de sécurité de système définis. Les responsables des projets de TI doivent planifier cette activité dans le cadre des activités de projet liées aux bornes de la phase d'analyse des besoins de leur CDS.

3.5 Phase de conception de haut niveau

Cette sous-section décrit les activités du PASSI de la phase de conception de haut niveau du CDS, qui font partie de la phase de développement ou d'acquisition du CVS.

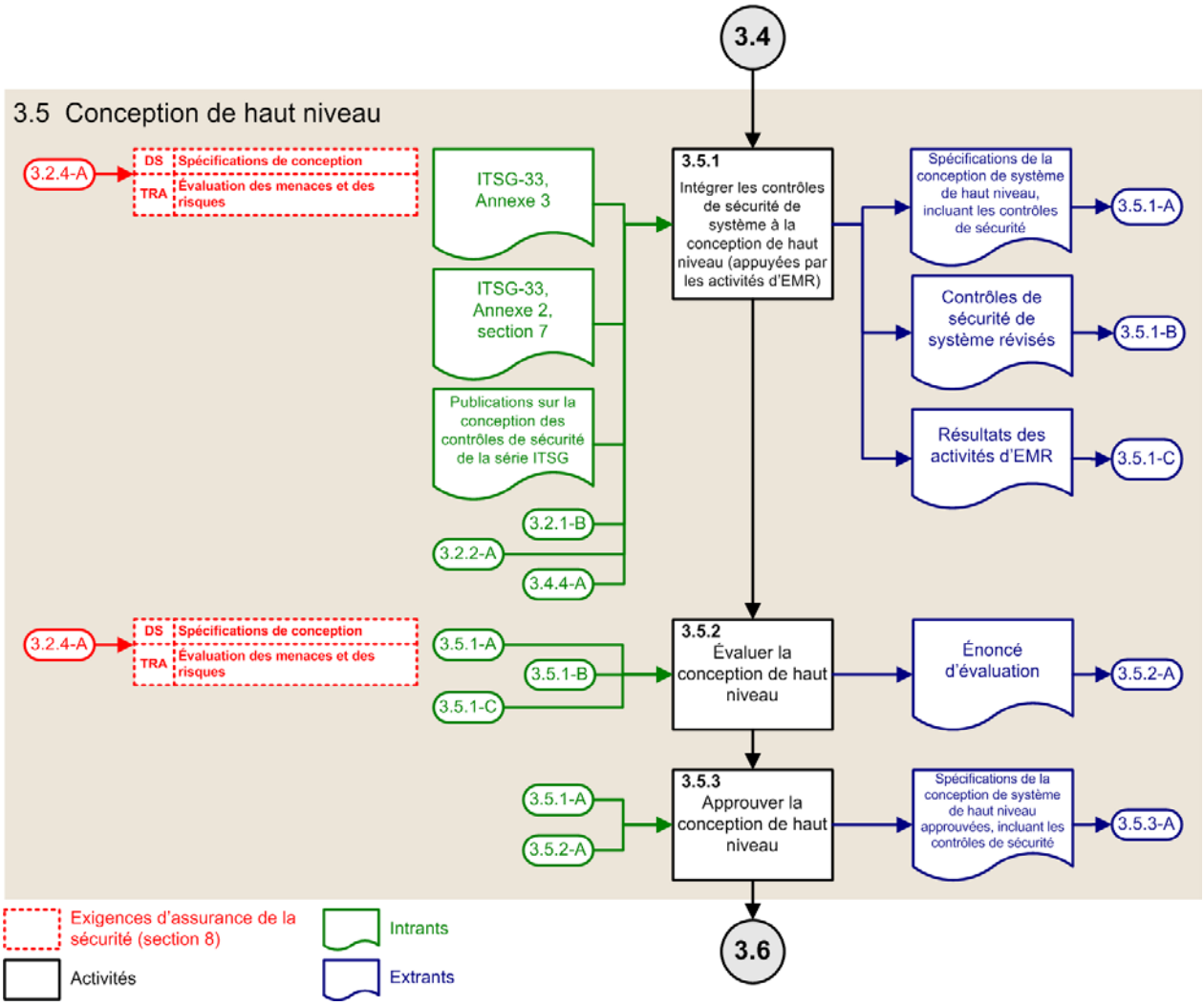


Figure 6 : Activités du PASSI – Phase de conception de haut niveau

3.5.1 Intégrer les contrôles de sécurité de système à la conception de haut niveau

Objectifs :	Intégrer les contrôles de sécurité de système à la conception de haut niveau du système d'information.
Rôle principal :	Concepteur de systèmes
Rôles de soutien :	Praticien de la sécurité et intégrateur de systèmes
Intrants :	ITSG-33, Annexe 3 – *Catalogue des contrôles de sécurité* [Référence 7] ITSG-33, Annexe 2, section 7 – *Déterminer le niveau de robustesse* [le présent document] Publications sur la conception des contrôles de sécurité de la série ITSG (p. ex., ITSG-31 – *Guide sur l'authentification des utilisateurs pour les systèmes TI* [Référence 8]) (3.2.1-B) Rapports d'évaluation des menaces de domaine pertinents (3.2.2-A) Rapport sur la catégorisation de la sécurité du système d'information (à l'appui de l'évaluation de la sensibilité du bien de TI; fait partie des activités d'EMR) (3.4.4-A) Contrôles de sécurité de système approuvés
Extrants :	(3.5.1-A) Spécifications de la conception de système de haut niveau, incluant les contrôles de sécurité (3.5.1-B) Contrôles de sécurité de système révisés (3.5.1-C) Résultats des activités d'EMR
Exigences relatives à l'assurance de la sécurité :	(3.2.4-A) Tâches techniques et exigences relatives au contenu des documents d'assurance de la sécurité pour les spécifications de conception (section 8, DS-E et DS-D) (3.2.4-A) Tâches techniques et exigences relatives au contenu des documents d'assurance de la sécurité pour l'EMR (section 8, TRA-E et TRA-D)

Lignes directrices :

Durant la phase de conception de haut niveau (parfois appelée conception d'architecture, conception de système ou conception logique), les responsables des projets de TI attribuent les contrôles de sécurité techniques, opérationnels et de gestion du système d'information aux éléments de la conception de système de haut niveau. Ce processus d'attribution n'est pas spécifiquement associé à la sécurité et suit normalement le processus standard d'ingénierie de système qui attribue les exigences aux éléments de la conception de système de haut niveau. En plus de l'attribution, les responsables précisent un niveau de robustesse approprié à chaque contrôle (ou à l'ensemble des contrôles qui exigent le même niveau de robustesse) pour orienter le travail qui suit la conception détaillée et s'assurer de la sélection des mécanismes et des solutions de sécurité de TI les plus pertinents. Voir les directives concernant la robustesse à la section 7.

Durant le processus de conception de haut niveau, le concepteur de systèmes et les praticiens de la sécurité peuvent effectuer d'autres travaux d'adaptation des contrôles lorsqu'ils envisagent différentes approches de conception de la sécurité et évaluent les menaces et les risques. La section 3.5.1.1 inclut d'autres directives de même nature qui tiennent compte des approches de conception et des activités d'EMR. Les procédures d'adaptation des contrôles sont décrites à la section 9.

3.5.1.1 Entreprendre les activités d'EMR

Le processus de conception de haut niveau s'appuie sur les activités d'EMR, elles-mêmes basées sur les résultats de l'évaluation des menaces de domaine concernée (le cas échéant) ou sur celle des menaces ministérielles. Le but de ces activités est en partie d'établir une base pour justifier l'ajout ou la suppression de contrôles (en utilisant l'Annexe 3 du guide ITSG-33 [Référence 7]) et d'en préciser les niveaux de robustesse afin d'évaluer l'environnement de menace de manière rentable.

Dans le PASSI, les activités d'EMR constituent un composant essentiel de l'ingénierie de la sécurité des systèmes d'information. Pour un projet de TI, le processus d'EMR est un outil de soutien des activités de conception de système. Les concepteurs et les praticiens utilisent le processus d'EMR pour :

- tenir compte de la sensibilité et des menaces liées aux biens de TI au moment de déterminer les composants système et leurs interactions et de sélectionner des mécanismes de sécurité;
- évaluer la mesure dans laquelle les contrôles et les mécanismes de sécurité arrivent à atténuer adéquatement les menaces;
- tenir compte des coûts et des avantages liés à la sécurité;
- ajuster les spécifications de conception suivant les résultats de l'évaluation;
- documenter les scénarios de risque;
- évaluer et signaler les risques résiduels aux intervenants de la sécurité.

Au moment de créer des systèmes d'information, il est préférable de mener les activités d'EMR comme un processus itératif. La Figure 7 illustre cette approche. On s'assure ainsi de tenir compte de manière efficace des menaces, des vulnérabilités et de leurs incidences au moment de prendre des décisions liées à la conception.

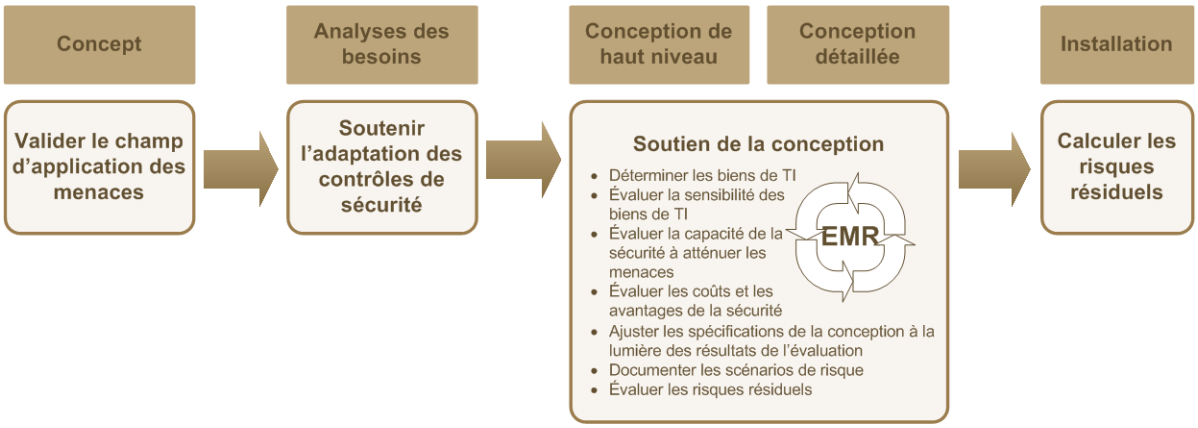


Figure 7 : Activités d'EMR dans le PASSI

On recommande aux concepteurs de systèmes et aux praticiens de la sécurité de documenter les résultats des activités d'EMR dans des produits livrables de projet habituels tout au long de la phase de conception de haut niveau, de la phase de conception détaillée et de la phase d'intégration et de test. La création d'un rapport d'EMR séparé n'est ni recommandée, ni nécessaire. Par contre, s'il faut consolider les résultats des activités d'EMR dans un rapport, on recommande de le faire durant l'évaluation des risques résiduels (section 3.9.3).

Durant la phase de conception de haut niveau, le but des activités d'EMR est d'aider les concepteurs et les praticiens à concevoir un système d'information capable de protéger adéquatement les biens de TI contre certaines menaces en utilisant l'ensemble actuel de contrôles et toute adaptation de contrôles supplémentaire jugée nécessaire. Les contrôles doivent être suffisamment robustes, et appliqués aux endroits appropriés durant la conception du système, pour protéger adéquatement les biens de TI contre les menaces qui se manifesteront dans l'environnement opérationnel.

À ce stade-ci, au cours de l'adaptation des contrôles, les responsables des projets de TI doivent respecter les approches de sécurité décrites dans le profil de contrôle de sécurité de domaine applicable puisqu'il faut rationaliser les contrôles pour tenir compte de leurs interrelations.

> Aux fins d'illustration, prenons l'exemple des utilisateurs finaux qui doivent interagir avec un système d'information qui traite de l'information protégée à la fois au travail, dans des ordinateurs de bureau, et à l'extérieur, dans des ordinateurs bloc-notes.
>
> Le profil applicable de contrôle de sécurité de domaine pour ce système d'information impose la sécurisation de l'information inactive (p. ex., le chiffrement des disques rigides) pour protéger les données sensibles et le contrôle d'accès physique (p. ex., une *zone de travail*) et surveiller l'accès aux ordinateurs de bureau. Dans ce scénario, la protection de l'information inactive peut être appliquée aux dispositifs mobiles (p. ex., les ordinateurs bloc-notes) afin de réduire l'incidence du vol de ces appareils. Dans le cas des dispositifs fixes (p. ex., les ordinateurs de bureau), la protection inhérente à la *zone de travail* permet de réduire de manière significative le risque d'exposition des données protégées stockées localement.
>
> Dans cet exemple, l'exigence d'un contrôle de sécurité visant à protéger les données inactives devient inutile pour obtenir un risque résiduel acceptable pour les ordinateurs de bureau. Cette rationalisation des contrôles permet aux responsables d'optimiser la sécurité, de réduire les coûts de développement et des opérations et d'accroître la convivialité.

Comme il est documenté à l'Annexe 1 du guide ITSG-33 [Référence 1], les ministères effectuent une évaluation des menaces ou des évaluations de menaces de domaine pour appuyer les projets de TI. Cette approche améliore grandement la qualité des données sur les menaces et réduit les efforts que les responsables doivent consentir aux activités d'EMR durant le CDS.

Les responsables des projets de TI doivent demander au coordonnateur de leur ministère de leur indiquer le processus d'EMR qu'ils doivent suivre.

3.5.1.2 Déterminer les niveaux de robustesse des contrôles de sécurité

Durant les activités d'EMR, les concepteurs de systèmes et les praticiens de la sécurité analysent les menaces et la sensibilité des biens de TI du système d'information et attribuent des contrôles de sécurité aux éléments de la conception de haut niveau afin de les protéger de manière adéquate. La sensibilité des biens de TI est équivalente à la catégorie de sécurité (et donc aux niveaux de préjudice) des activités

opérationnelles prises en charge par chaque bien. Par exemple, un serveur d'applications qui participe au traitement d'une activité opérationnelle dont la catégorie de sécurité est cotée Protégé B, intégrité et disponibilité moyennes, héritera du niveau de sensibilité coté Protégé B, intégrité et disponibilité moyennes. Les praticiens précisent également les niveaux de robustesse des contrôles qui aideront les responsables de la conception détaillée à choisir les mécanismes de sécurité appropriés. Bien qu'elle ne soit pas requise au sens strict, cette étape permet d'offrir des conseils utiles aux concepteurs et est donc recommandée.

Le PASSI utilise la robustesse pour indiquer la force et l'assurance requises des contrôles en place pour assurer une protection adéquate contre certaines menaces susceptibles de compromettre la confidentialité, l'intégrité et la disponibilité des biens de TI. Les contrôles qui protègent les biens de TI plus sensibles (c.-à-d. ceux qui prennent en charge des activités opérationnelles dont le niveau des préjudices prévus est plus élevé) ou qui sont exposés à des menaces plus importantes (p. ex., à des agents de menace qui ont des capacités plus sophistiquées) doivent être plus forts et posséder un niveau d'assurance plus élevé et exigent donc des niveaux de robustesse plus élevés. Le modèle de robustesse est décrit à la section 7.

L'analyse de la catégorie de sécurité du système d'information effectuée précédemment, le contexte de menace et les approches de sécurité décrites dans le profil de contrôle de sécurité applicable, ainsi que l'information supplémentaire sur les menaces, documentée dans les rapports d'évaluation des menaces du ministère ou de domaine (s'il y a lieu), permettent de déterminer des niveaux de robustesse rentables et aptes à répondre aux besoins opérationnels.

Les approches de sécurité décrites dans le profil applicable de contrôle de sécurité de domaine peuvent également influer sur la spécification des niveaux de robustesse compte tenu de la protection offerte par les interrelations entre les contrôles de sécurité.

> À titre d'exemple, un système d'information protégé par des contrôles de frontières stricts (forte confidentialité de la transmission, forte authentification des sources, etc.), une sécurité matérielle forte (barrières, agents de sécurité, etc.) et une bonne sécurité du personnel (cote de sécurité) peut tolérer des contrôles de sécurité internes moins robustes (p. ex., des contrôles de vérification et de responsabilisation habituels). Toutefois, cette approche exige de mettre davantage l'accent sur certains contrôles importants, qui doivent être surveillés plus étroitement afin de s'assurer qu'ils réduisent effectivement la menace interne à un niveau acceptable. Par exemple, si l'expérience passée (p. ex., une fraude interne) indique que la menace interne est plus sérieuse qu'initialement prévue, les responsables doivent envisager des contrôles internes plus robustes (p. ex., authentification forte et contrôles de vérification et de responsabilisation stricts).

D'autre part, les niveaux de robustesse ont une influence sur les exigences d'assurance de la sécurité applicables aux projets de TI. Des niveaux plus élevés attribués à un ensemble de contrôles exigent l'application d'exigences d'assurance plus strictes durant la conception, le développement, les tests et l'exploitation de ces contrôles.

> Puisque la sélection du niveau de robustesse a une incidence sur les coûts, les responsables des projets voudront peut-être tenir compte d'autres facteurs au moment de la sélection. Par exemple, il peut ne pas être rentable pour un ministère de protéger une activité opérationnelle particulière contre des menaces sophistiquées (p. ex., des services de renseignement étrangers très motivés qui lancent des attaques ciblées, le crime organisé qui compromet des employés) lorsqu'il est établi que les agents de menace visent essentiellement d'autres cibles au sein de

l'organisme. Dans cet exemple, les responsables du ministère peuvent opter pour un niveau de robustesse inférieur (c.-à-d., qui ne protégera pas nécessairement le système d'information contre des menaces sophistiquées) et en accepter les risques. L'acceptation du risque est donc explicite dès les premières phases de développement du système. Quoi qu'il en soit, la sélection d'un niveau de robustesse différent de celui recommandé à la section 7 doit être justifiée et suffisamment documentée.

Le niveau de robustesse des contrôles et les exigences d'assurance connexes peuvent être ajustés ultérieurement durant la phase de conception détaillée du PASSI pour tenir compte des analyses de menaces plus précises et des choix de conception.

La section 7 donne des directives sur la détermination des niveaux de robustesse appropriés des contrôles en fonction de la sensibilité et de la catégorie de menace des biens de TI.

3.5.2 Évaluer la conception de haut niveau

Objectifs :	Confirmer que l'attribution des contrôles de sécurité lors de la conception de haut niveau a été effectuée en conformité avec les exigences d'assurance de la sécurité.
Rôle principal :	Évaluateur de la sécurité
Rôles de soutien :	Praticien de la sécurité
Intrants :	(3.5.1-A) Spécifications de la conception de système de haut niveau, incluant les contrôles de sécurité (3.5.1-B) Contrôles de sécurité de système révisés (3.5.1-C) Résultats des activités d'EMR
Extrants :	(3.5.2-A) Énoncé d'évaluation de la conception de système de haut niveau.
Exigences relatives à l'assurance de la sécurité :	(3.2.4-A) Tâches d'évaluation d'assurance de la sécurité pour la spécification de conception (section 8, DS-A) (3.2.4-A) Tâches d'évaluation d'assurance de la sécurité pour l'EMR (section 8, TRA-A)

Lignes directrices :

De pair avec le praticien de la sécurité, l'évaluateur de la sécurité doit effectuer les tâches suivantes :

- Confirmer que les travaux de spécification de la conception de haut niveau respectent les tâches techniques et les exigences relatives au contenu des documents;
- Confirmer que les travaux d'EMR respectent les tâches techniques et les exigences relatives au contenu des documents;
- Préparer un énoncé d'évaluation aux fins d'approbation.

3.5.3 Approuver la conception de haut niveau

Objectifs :	Obtenir l'autorisation de commencer la conception détaillée du système d'information selon les spécifications de la conception de haut niveau.
Rôle principal :	Autorisateur
Rôles de soutien :	Évaluateur de la sécurité
Intrants :	(3.5.1-A) Spécifications de la conception de système de haut niveau, incluant les contrôles de sécurité (3.5.2-A) Énoncé d'évaluation de la conception de système de haut niveau
Extrants :	(3.5.3-A) Spécifications de la conception de système de haut niveau approuvées, incluant les contrôles de sécurité
Exigences relatives à l'assurance de la sécurité :	Aucune exigence particulière

Lignes directrices :

Cette activité est recommandée pour les grands projets de TI et au moment de mettre en œuvre des systèmes d'information qui servent à soutenir des activités opérationnelles plus critiques; elle peut être omise pour les plus petits projets et les systèmes d'information moins critiques.

Les responsables des projets de TI doivent planifier cette activité dans le cadre des activités de projet liées aux bornes de la phase de conception de haut niveau du CDS.

Le but principal de cette activité est d'obtenir l'approbation de l'autorisateur de commencer la phase de conception détaillée du projet en utilisant les spécifications de la conception de haut niveau. Elle permet également à l'autorisateur et aux autres intervenants de la sécurité d'examiner et d'approuver les autres extrants du PASSI de la phase de conception de haut niveau avant d'accorder la permission de poursuivre le projet. Les responsables des projets de TI doivent tenir compte de ce qui suit :

- Examiner, avec l'autorisateur et les agents de sécurité du ministère, les résultats des activités d'EMR de la phase de conception de haut niveau, particulièrement les décisions et les justifications concernant la réduction ou l'augmentation des contrôles;
- Examiner, avec les agents de sécurité du ministère, les contrôles de sécurité de système révisés.

3.6 Phase de conception détaillée

Cette sous-section décrit les activités du PASSI de la phase de conception détaillée du CDS, qui font partie de la phase de développement ou d'acquisition du CVS.

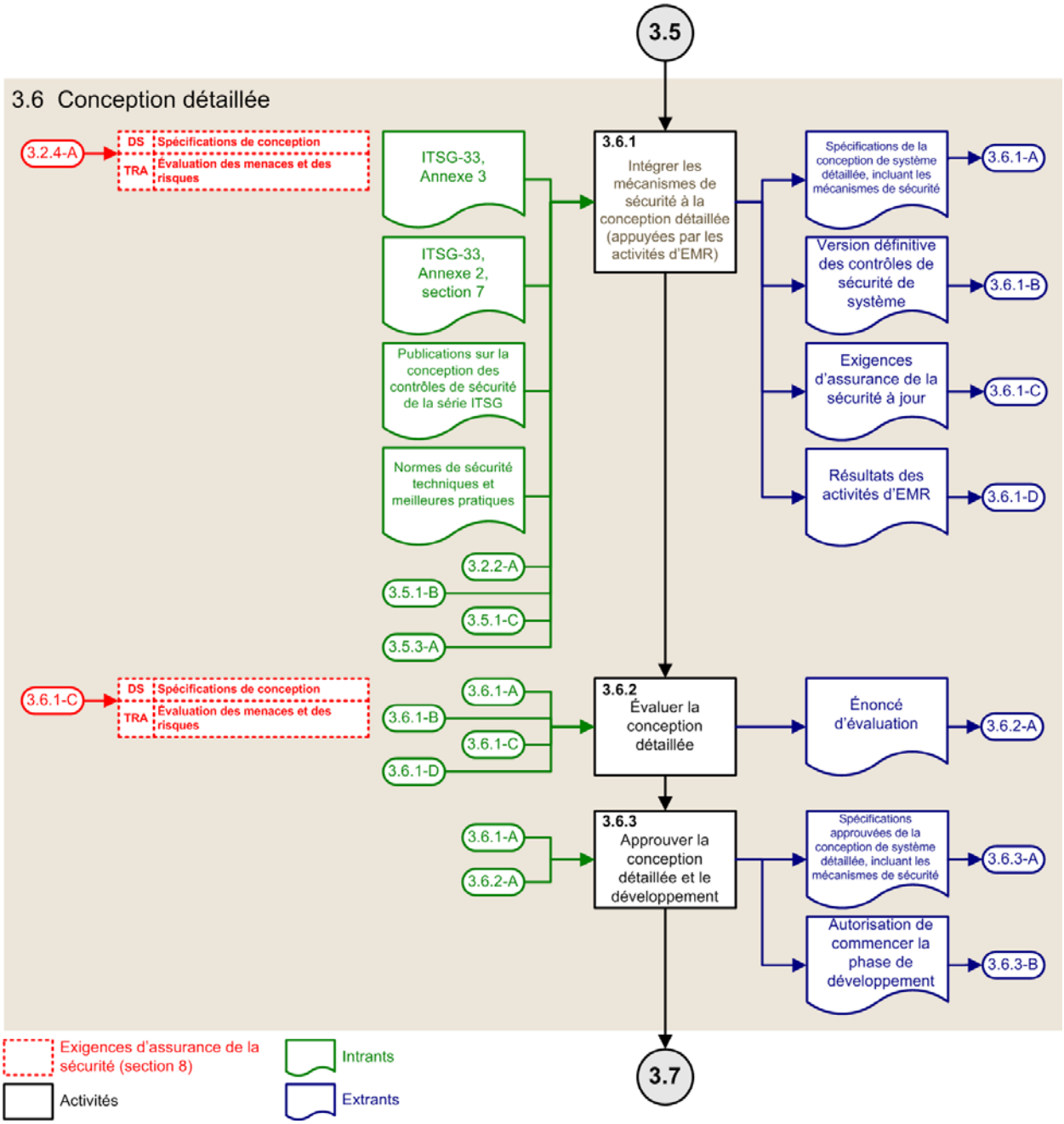


Figure 8 : Activités du PASSI – Phase de conception détaillée

3.6.1 Intégrer les mécanismes de sécurité à la conception détaillée

Objectifs :	Répondre aux exigences de contrôle de la sécurité de la conception détaillée du système d'information en attribuant des mécanismes de sécurité appropriés aux éléments de la conception.
Rôle principal :	Concepteur de systèmes
Rôles de soutien :	Praticien de la sécurité et intégrateur de systèmes
Intrants :	ITSG-33, Annexe 3 – *Catalogue des contrôles de sécurité* [Référence 7] ITSG-33, Annexe 2, section 7 – *Déterminer le niveau de robustesse* [le présent document] Publications sur la conception des contrôles de sécurité de la série ITSG (p. ex., ITSG-31 – *Guide sur l'authentification des utilisateurs pour les systèmes TI* [Référence 8]) Normes de sécurité techniques et meilleures pratiques du gouvernement et de l'industrie (3.2.2-A) Rapport sur la catégorisation de la sécurité du système d'information (à l'appui de l'évaluation de la sensibilité du bien de TI; fait partie des activités d'EMR) (3.5.1-B) Contrôles de sécurité de système révisés (3.5.1-C) Résultats des activités d'EMR (de la phase précédente) (3.5.3-A) Spécifications de la conception de système de haut niveau approuvées, incluant les contrôles de sécurité
Extrants :	(3.6.1-A) Spécifications de la conception de système détaillée, incluant les mécanismes de sécurité (3.6.1-B) Version définitive des contrôles de sécurité de système (3.6.1-C) Exigences d'assurance de la sécurité à jour (3.6.1-D) Résultats des activités d'EMR
Exigences relatives à l'assurance de la sécurité :	(3.2.4-A) Tâches techniques et exigences relatives au contenu des documents d'assurance de la sécurité pour les spécifications de conception (section 8, DS-E et DS-D) (3.2.4-A) Tâches techniques et exigences relatives au contenu des documents d'assurance de la sécurité pour l'EMR (section 8, TRA-E et TRA-D)

Lignes directrices :

Durant la phase de conception détaillée, les responsables des projets de TI attribuent des mécanismes de sécurité aux éléments de la conception détaillée pour satisfaire aux contrôles de sécurité précisés dans les spécifications de la conception de système de haut niveau. Le processus de conception détaillée ne

concerne pas spécifiquement la sécurité et doit suivre le processus habituel d'ingénierie de système pour transformer les spécifications de la conception de haut niveau en spécifications de conception détaillée.

3.6.1.1 Entreprendre les activités d'EMR

Durant la phase de conception détaillée, les activités d'EMR offrent des justifications, basées sur les risques, pour sélectionner des mécanismes de sécurité dotés d'une force suffisante pour protéger les composants du système d'information contre les menaces. La conception de haut niveau précise les niveaux de robustesse requis pour les contrôles. Notons que les publications de la série ITSG, tel le guide ITSG-31 – *Guide sur l'authentification des utilisateurs pour les systèmes TI* [Référence 8], incluent des lignes directrices sur la sélection des mécanismes de sécurité pour les contrôles, p. ex., l'authentification basée sur les niveaux de robustesse.

La force des mécanismes de sécurité doit être suffisante, et appliquée à l'étape appropriée de la conception détaillée, pour protéger adéquatement les biens de TI contre les risques qui les menacent dans l'environnement opérationnel du système d'information. Les activités d'EMR peuvent donner lieu à des changements dans la façon de sélectionner les contrôles pour régler les problèmes de sécurité liés à la conception détaillée. Si des changements sont effectués, les extrants des contrôles de sécurité de système doivent être modifiés en conséquence.

On recommande aux concepteurs et aux praticiens de la sécurité de documenter les résultats des activités d'EMR dans des produits livrables de projet habituels tout au long de la phase de conception de haut niveau, la phase de conception détaillée et de la phase d'intégration et de test.

Tout changement apporté aux niveaux de robustesse précisés à ce stade peut entraîner des changements dans les exigences d'assurance de la sécurité. Les responsables des projets de TI doivent examiner ces changements avec soins puisqu'ils peuvent entraîner des coûts et des délais supplémentaires lorsque les phases d'analyse des besoins ou de conception de haut niveau du CDS doivent être reprises, en tout ou en partie, pour tenir compte des nouvelles exigences d'assurance de la sécurité. Si des changements sont effectués, les extrants des contrôles de sécurité de système doivent être modifiés en conséquence.

La section 9 renferme des procédures d'adaptation des contrôles de sécurité.

3.6.2 Évaluer la conception détaillée

Objectifs :	Confirmer que la spécification des mécanismes de sécurité de la conception détaillée a été effectuée en conformité avec les exigences d'assurance de la sécurité.
Rôle principal :	Évaluateur de la sécurité
Rôles de soutien :	Praticien de la sécurité
Intrants :	(3.6.1-A) Spécifications de la conception de système détaillée, incluant les mécanismes de sécurité (3.6.1-B) Version définitive des contrôles de sécurité de système (3.6.1-C) Exigences d'assurance de la sécurité à jour (3.6.1-D) Résultats des activités d'EMR
Extrants :	(3.6.2-A) Énoncé d'évaluation de la conception de système détaillée
Exigences relatives à l'assurance de la sécurité :	(3.6.1-C) Tâches d'évaluation d'assurance de la sécurité pour la spécification de la conception (section 8, DS-A) (3.6.1-C) Tâches d'évaluation d'assurance de la sécurité pour l'EMR (section 8, TRA-A)

Lignes directrices :

De pair avec le praticien de la sécurité, l'évaluateur de la sécurité doit exécuter les tâches suivantes :

- Confirmer que les travaux liés à la spécification de la conception détaillée respectent les tâches techniques et les exigences relatives au contenu des documents;
- Confirmer que les travaux d'EMR respectent les tâches techniques et les exigences relatives au contenu des documents;
- Préparer un énoncé d'évaluation aux fins d'approbation.

3.6.3 Approuver la conception détaillée et le développement

Objectifs :	Obtenir l'autorisation de commencer le développement du système d'information en fonction des spécifications de la conception détaillée.
Rôle principal :	Autorisateur
Rôles de soutien :	Évaluateur de la sécurité
Intrants :	(3.6.1-A) Spécifications de la conception de système détaillée, incluant les mécanismes de sécurité (3.6.2-A) Énoncé d'évaluation de la conception de système détaillée
Extrants :	(3.6.3-A) Spécifications approuvées de la conception de système détaillée, incluant les mécanismes de sécurité (3.6.3-B) Autorisation de commencer la phase de développement
Exigences relatives à l'assurance de la sécurité :	Aucune exigence particulière

Lignes directrices :

Le but principal de cette activité est d'obtenir de l'autorisateur l'approbation requise pour commencer le développement du système d'information selon les spécifications de la conception détaillée. Au besoin, les responsables des projets de TI doivent obtenir cette approbation avant d'établir l'environnement de développement et d'engager l'équipe responsable, éléments qui peuvent représenter des coûts importants dans le cadre du projet. L'activité permet également à l'autorisateur et aux autres intervenants de la sécurité d'examiner et d'approuver les autres extrants du PASSI de la phase de conception détaillée avant d'accorder la permission de continuer le projet. Les responsables des projets de TI doivent tenir compte de ce qui suit :

- Examiner, avec l'autorisateur et les agents de sécurité du ministère, les résultats des activités d'EMR de la phase de conception détaillée, particulièrement les décisions et les justifications concernant la réduction ou l'augmentation des contrôles de sécurité et la sélection des mécanismes de sécurité;
- Examiner, avec les agents de sécurité du ministère, les contrôles de sécurité définitifs propres au système;
- Examiner, avec l'autorisateur et les agents de sécurité du ministère, tous les changements apportés aux exigences d'assurance de la sécurité pour le reste des activités de sécurité.

Les responsables des projets de TI doivent planifier cette activité dans le cadre des activités de projet liées aux bornes de la phase de conception détaillée du CDS.

L'autorisation de commencer le développement du système peut être aussi simple qu'un compte rendu de décision d'un procès-verbal d'une réunion technique ou de projet, ou aussi formelle qu'une lettre d'autorisation signée par l'autorisateur.

3.7 Phase de développement

Cette sous-section décrit les activités du PASSI de la phase de développement du CDS, qui font partie de la phase de développement ou d'acquisition du CVS.

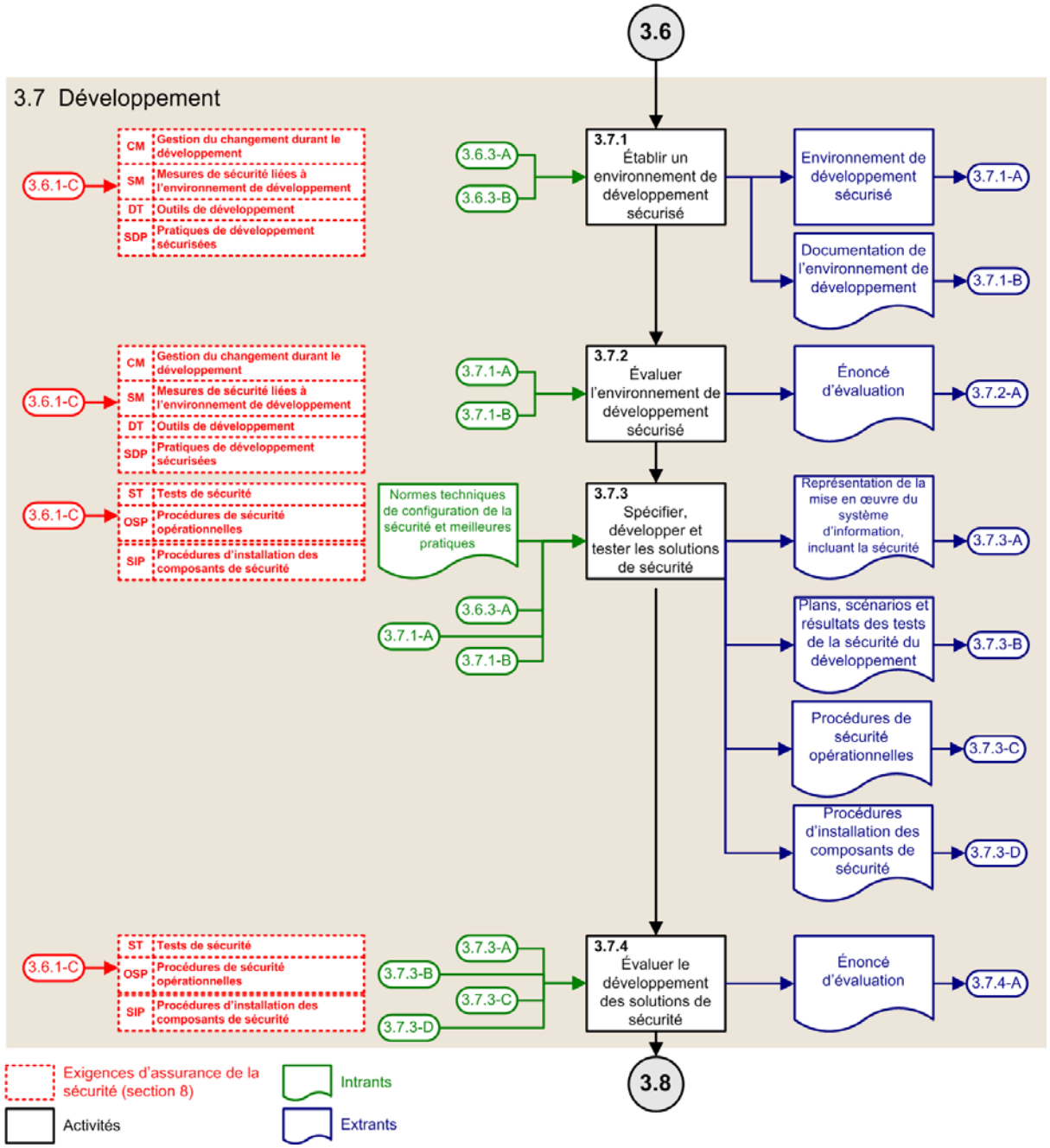


Figure 9 : Activités du PASSI – Phase de développement

3.7.1 Établir un environnement de développement sécurisé

Objectifs :	Établir un environnement de développement sécurisé pour appuyer le développement du système d'information et de sa sécurité.
Rôle principal :	Développeur de systèmes
Rôles de soutien :	Praticien de la sécurité
Intrants :	(3.6.3-A) Spécifications approuvées de la conception de système détaillée, incluant les mécanismes de sécurité (3.6.3-B) Autorisation de commencer la phase de développement
Extrants :	(3.7.1-A) Environnement de développement sécurisé (3.7.1-B) Documentation de l'environnement de développement
Exigences relatives à l'assurance de la sécurité :	(3.6.1-C) Tâches techniques et exigences relatives au contenu des documents d'assurance de la sécurité pour la gestion du changement durant le développement (section 8, CM-E et CM-D) (3.6.1-C) Tâches techniques et exigences relatives au contenu des documents d'assurance de la sécurité pour les mesures de sécurité liées à l'environnement de développement (section 8, SM-E et SM-D) (3.6.1-C) Tâches techniques et exigences relatives au contenu des documents d'assurance de la sécurité pour les outils de développement (section 8, DT-E et DT-D) (3.6.1-C) Tâches techniques et exigences relatives au contenu des documents d'assurance de la sécurité pour les pratiques de développement sécurisées (section 8, SDP-E et SDP-D)

Lignes directrices :

Les exigences d'assurance de la sécurité dictent dans une large mesure les efforts que les responsables d'un projet de TI doivent consacrer à l'établissement d'un environnement et de pratiques de développement sécurisés appropriés. Pour éviter les vulnérabilités et les faiblesses liées à la sécurité dans les systèmes d'information, les exigences imposent de recourir à de saines pratiques de développement et d'approvisionnement non seulement pour les solutions de sécurité, mais pour tous les aspects du système d'information. Les efforts consentis pour établir la qualité, la fiabilité et la résilience du logiciel et du matériel contribuent tous au développement de systèmes d'information fiables, que les efforts soient orientés ou non vers la sécurité.

Les pratiques de développement et d'approvisionnement qui appuient la mise en œuvre de systèmes d'information fiables incluent, sans s'y limiter, les éléments suivants :

- Principes et méthodologies de l'ingénierie de sécurité;
- Pratiques liées au codage sécurisé;
- Utilisation de normes sur la sécurité du langage;

- Utilisation d'outils et de techniques d'analyse du code source;
- Utilisation d'outils et de techniques d'analyse binaire;
- Examen du code source;
- Signature du code;
- Utilisation d'outils de test commerciaux ou de source ouverte;
- Sélection de produits commerciaux validés en fonction des critères de sécurité (p. ex., normes FIPS pour les modules cryptographiques, Critères communs pour les produits);
- Recours à des fournisseurs de logiciels et de matériel de confiance.

3.7.2 Évaluer l'environnement de développement sécurisé

Objectifs :	Confirmer que l'environnement de développement sécurisé a été établi en conformité avec les exigences d'assurance de la sécurité.
Rôle principal :	Évaluateur de la sécurité
Rôles de soutien :	Praticien de la sécurité
Intrants :	(3.7.1-A) Environnement de développement sécurisé (3.7.1-B) Documentation de l'environnement de développement
Extrants :	(3.7.2-A) Énoncé d'évaluation de l'environnement de développement sécurisé
Exigences relatives à l'assurance de la sécurité :	(3.6.1-C) Tâches d'évaluation d'assurance de la sécurité pour la gestion du changement durant le développement (section 8, CM-A) (3.6.1-C) Tâches d'évaluation d'assurance de la sécurité pour les mesures de sécurité liées à l'environnement de développement (section 8, SM-A) (3.6.1-C) Tâches d'évaluation d'assurance de la sécurité pour les outils de développement (section 8, DT-A) (3.6.1-C) Tâches d'évaluation d'assurance de la sécurité pour les pratiques de développement sécurisé (section 8, SDP-A)

Lignes directrices :

De pair avec le praticien de la sécurité, l'évaluateur de la sécurité doit effectuer les tâches suivantes :

- Confirmer que les travaux liés à l'établissement de l'environnement de développement respectent les tâches techniques et les exigences relatives au contenu des documents;
- Préparer un énoncé d'évaluation aux fins d'approbation.

3.7.3 Préciser, développer et tester les solutions de sécurité

Objectifs :	Préciser les solutions de sécurité qui permettront d'appliquer les mécanismes de sécurité indiqués dans les spécifications de la conception détaillée, développer des composants de sécurité adaptés et acquérir les composants disponibles dans le commerce. Appliquer des pratiques sécurisées à tous les aspects des activités de développement du système d'information.
Rôle principal :	Développeur de systèmes, intégrateur de systèmes et testeur de systèmes
Rôles de soutien :	Praticien de la sécurité
Intrants :	Normes techniques de configuration de la sécurité et meilleures pratiques (3.6.3-A) Spécifications approuvées de la conception de système détaillée, incluant les mécanismes de sécurité (3.7.1-A) Environnement de développement sécurisé (3.7.1-B) Documentation de l'environnement de développement
Extrants :	(3.7.3-A) Représentation de la mise en œuvre du système d'information, incluant la sécurité (y compris la nomenclature et les paramètres de configuration de la sécurité) (3.7.3-B) Plans, scénarios et résultats des tests de la sécurité du développement (3.7.3-C) Procédures de sécurité opérationnelles (3.7.3-D) Procédures d'installation des composants de sécurité
Exigences relatives à l'assurance de la sécurité :	(3.6.1-C) Tâches techniques et exigences relatives au contenu des documents d'assurance de la sécurité pour les tests de sécurité (section 8, ST-E et ST-D) (3.6.1-C) Tâches techniques et exigences relatives au contenu des documents d'assurance de la sécurité pour les procédures de sécurité opérationnelles (section 8, OSP-E et OSP-D) (3.6.1-C) Tâches techniques et exigences relatives au contenu des documents d'assurance de la sécurité pour les procédures d'installation des composants de sécurité (section 8, SIP-E et SIP-D)

Lignes directrices :

Les activités de développement respectent les pratiques de développement sécurisées mises en place pour l'environnement de développement sécurisé, conformément aux exigences d'assurance de la sécurité. Les pratiques prescrites s'appliquent non seulement au développement des solutions de sécurité, mais à l'ensemble du système (p. ex., les pratiques liées au codage sécurisé, qui s'appliquent à tous les composants logiciels du système et non seulement aux composants de sécurité). Les mécanismes de sécurité peuvent être appliqués de plusieurs façons :

- Acquisition et installation de produits de sécurité commerciaux;
- Utilisation des mécanismes de sécurité inclus dans les produits commerciaux (non liés à la sécurité);
- Configuration sécurisée des produits commerciaux;
- Codage des contrôles de sécurité sous forme de programmes logiciels discrets;
- Insertion d'un contrôle de sécurité sous forme de code dans un autre code logiciel;
- Acquisition d'une capacité externe (c.-à-d. la capacité d'un fournisseur externe);
- Spécification d'une procédure de sécurité opérationnelle (voir la section 3.7.3.1);
- Spécification d'une procédure d'installation des composants de sécurité (voir la section 3.7.3.3).

Au fur et à mesure que progressent les travaux de développement, les développeurs, avec l'aide des praticiens de la sécurité, doivent déterminer et examiner les paramètres de configuration du système qui s'appliquent à leurs choix technologiques. Par exemple, si un développeur choisit le protocole OpenSSL pour mettre en place un mécanisme de sécurité pour le chiffrement de session, il doit indiquer les paramètres de configuration de la sécurité qui correspondent aux normes ou aux meilleures pratiques de configuration applicables. Il doit préciser tous ces paramètres et inclure les spécifications correspondantes dans la représentation de la mise en œuvre du système d'information. La mise en œuvre des paramètres peut ensuite être évaluée durant la phase d'installation du CDS.

Tous les tests qui peuvent être effectués au cours des travaux de développement et qui contribuent à l'établissement de l'assurance de la sécurité sont inclus dans cette activité. Ces tests incluent les tests fonctionnels des solutions de sécurité personnalisées (p. ex., test d'unité fonctionnel) et peuvent également inclure d'autres formes de tests tels les tests fonctionnels inversés des fonctions non liées à la sécurité (p. ex., les tests à données aléatoires d'une URL dans une application Web). Ils peuvent également inclure les tests des procédures opérationnelles pour en déterminer la convivialité et la maintenabilité.

Les développeurs doivent produire des plans, des scénarios et des résultats de tests de la sécurité du développement aux fins d'assurance de la sécurité.

Les aspects liés à la sécurité mentionnés dans les lignes directrices sur la passation de marchés peuvent influer sur l'acquisition de solutions commerciales de plusieurs façons. Par exemple, certaines pratiques peuvent exiger le recours à des sources fiables pour l'acquisition de logiciels.

La représentation de la mise en œuvre du système d'information, incluant la sécurité, est le principal extrant de la phase de développement. Elle est la moins abstraite des représentations du système d'information. Elle inclut le code source, les produits matériels et logiciels, les diagrammes du réseau physique, la documentation de configuration tels les manuels de construction, et ainsi de suite. Collectivement, ces éléments permettent de créer le système sans qu'il soit nécessaire de prendre quelque décision que ce soit relativement à la conception ou à la mise en œuvre.

3.7.3.1 Tests de sécurité fonctionnels

Les tests de sécurité de cette phase du CDS incluent les tests fonctionnels. Le but de ces tests est de valider la fonctionnalité des mécanismes de sécurité appliqués par les solutions de sécurité.

Lors de la préparation des scénarios de test, les développeurs doivent s'assurer de tester de façon appropriée la fonctionnalité de chaque mécanisme de sécurité et voir à ce que chaque test établisse clairement sa correspondance aux mécanismes de sécurité qu'il valide. Comme il est indiqué à la section 3.4.2.1, les développeurs peuvent utiliser une MTES pour établir cette correspondance. Si cette matrice est utilisée, les testeurs peuvent la mettre à jour en utilisant les résultats réels obtenus au fur et à mesure du déroulement des tests de sécurité. Ainsi, les responsables obtiennent une MTES qui permet une traçabilité amont complète, des scénarios de test aux éléments de conception et aux besoins opérationnels.

3.7.3.2 Procédures de sécurité opérationnelles

Pour appuyer les opérations, les développeurs et les praticiens doivent produire un ensemble de procédures de sécurité opérationnelles qui garantissent l'exploitation, l'administration et la maintenance sécurisées du système durant sa période d'exploitation. Ces procédures font partie des dispositions relatives à la sécurité que les groupes responsables des opérations de TI doivent inclure dans leur plan d'exploitation.

En conformité avec les politiques et les normes ministérielles, les procédures de sécurité opérationnelles doivent tenir compte des éléments suivants :

- Politiques et procédures relatives à la sécurité des systèmes d'information;
- Aspects liés à la sécurité de la gestion du changement (incluant la gestion des rustines);
- Aspects liés à la sécurité de la gestion de la configuration;
- Aspects liés à la sécurité de la gestion des versions;
- Gestion des incidents;
- Planification d'urgence;
- Évaluations périodiques de la sécurité des systèmes d'information, telles les évaluations de vulnérabilités;
- Exigences relatives à la maintenance de la sécurité, telles les mises à jour de clés cryptographiques;
- Examen des menaces, des vulnérabilités et des risques;
- Examens et vérifications de la conformité aux exigences de sécurité;
- Rapports sur la gestion des risques;
- Aspects liés à la sécurité d'un plan d'élimination de système d'information.

Normalement, ces éléments sont couverts par des procédures de sécurité opérationnelles déjà prévues dans les contrôles de sécurité communs. Les responsables doivent communiquer avec le coordonnateur de la sécurité des TI de leur ministère afin de déterminer si ces procédures héritées des contrôles communs répondent aux contrôles de sécurité de système et de cerner celles qu'il faut développer dans le cadre du projet.

3.7.3.3 Procédures d'installation des composants de sécurité

Les développeurs de systèmes doivent produire des procédures d'installation des composants de sécurité pour le système. Ces procédures décrivent les étapes nécessaires pour installer et configurer correctement

les solutions de sécurité et définir les paramètres de configuration de la sécurité, incluant les procédures de renforcement, durant le processus d'installation et dans les activités de reprise après sinistre.

3.7.4 Évaluer le développement des solutions de sécurité

Objectifs :	Confirmer que le développement des solutions de sécurité et de l'ensemble du système d'information a été effectué en conformité avec les exigences d'assurance de la sécurité.
Rôle principal :	Évaluateur de la sécurité
Rôles de soutien :	Praticien de la sécurité
Intrants :	(3.7.3-A) Représentation de la mise en œuvre du système d'information, incluant la sécurité (3.7.3-B) Plans, scénarios et résultats des tests de la sécurité du développement (3.7.3-C) Procédures de sécurité opérationnelles (3.7.3-D) Procédures d'installation des composants de sécurité
Extrants :	(3.7.4-A) Énoncé d'évaluation du développement de la sécurité
Exigences relatives à l'assurance de la sécurité :	(3.6.1-C) Tâches d'évaluation d'assurance de la sécurité pour les tests de sécurité (section 8, ST-A) (3.6.1-C) Tâches d'évaluation d'assurance de la sécurité pour les procédures de sécurité opérationnelles (section 8, OSP-A) (3.6.1-C) Tâches d'évaluation d'assurance de la sécurité pour les procédures d'installation des composants de sécurité (section 8, SIP-A)

Lignes directrices :

De pair avec le praticien de la sécurité, l'évaluateur de la sécurité doit effectuer les tâches suivantes :

- Confirmer que les travaux liés aux tests de sécurité effectués pendant le développement respectent les tâches techniques et les exigences relatives au contenu des documents;
- Confirmer que les procédures de sécurité opérationnelles répondent aux exigences relatives au contenu des documents;
- Confirmer que les procédures d'installation des composants de sécurité répondent aux exigences relatives au contenu des documents;
- Préparer un énoncé d'évaluation aux fins d'approbation.

3.8 Phase d'intégration et de test

Cette sous-section décrit les activités du PASSI de la phase d'intégration et de test du CDS, qui font partie de la phase d'intégration et d'installation du CVS.

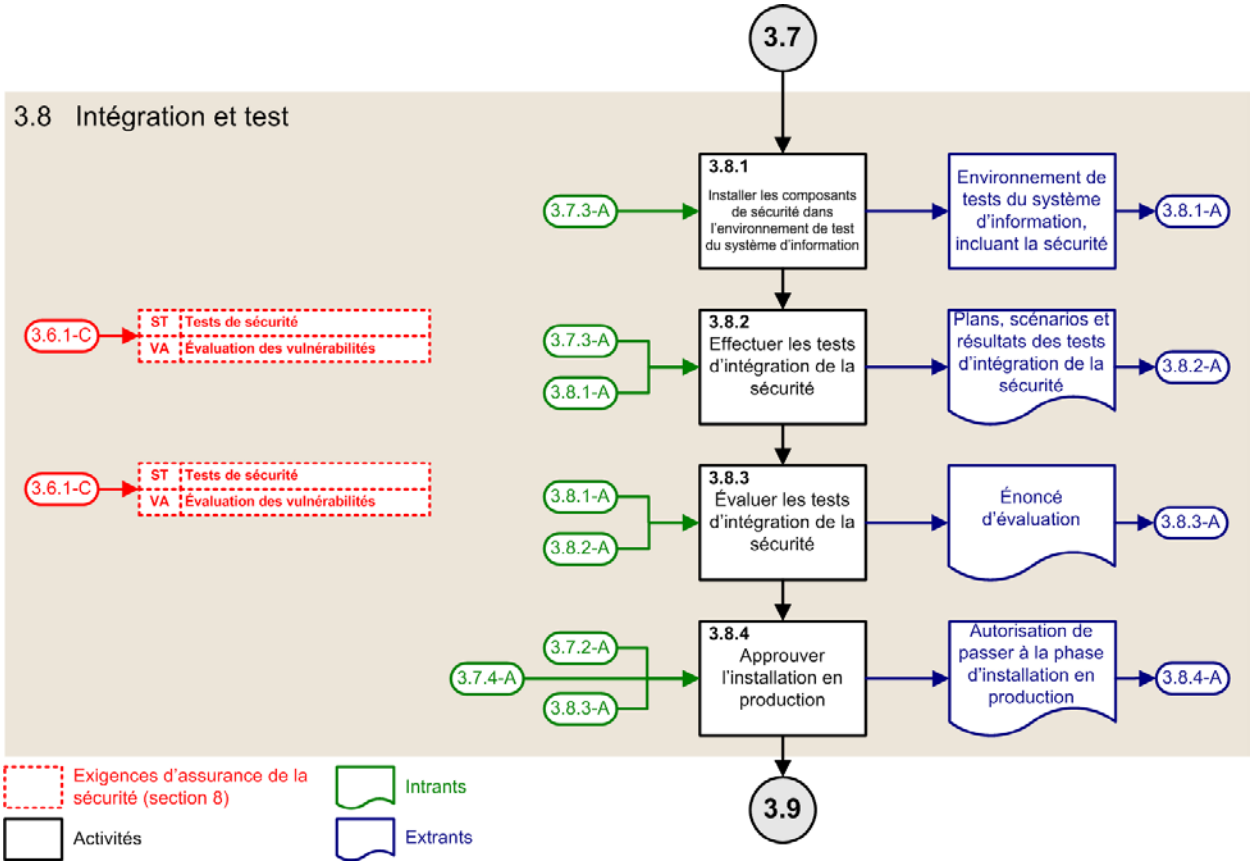


Figure 10 : Activités du PASSI – Phase d'intégration et de test

3.8.1 Installer les composants de sécurité dans l'environnement de test du système d'information

Objectifs :	Installer les composants de sécurité dans l'environnement de test du système d'information en conformité avec la représentation de la mise en œuvre du système d'information.
Rôle principal :	Intégrateur de systèmes
Rôles de soutien :	Praticien de la sécurité
Intrants :	(3.7.3-A) Représentation de la mise en œuvre du système d'information, incluant la sécurité
Extrants :	(3.8.1-A) Environnement de test du système d'information, incluant la sécurité
Exigences relatives à l'assurance de la sécurité :	Aucune exigence particulière

Lignes directrices :

Pour se préparer à effectuer les tests de sécurité, les responsables des projets de TI installent les composants de sécurité et appliquent la configuration de sécurité dans un ou plusieurs environnements de test. Les environnements doivent fournir les plates-formes qui permettent d'effectuer tous les tests de sécurité prescrits.

Notons que les projets de TI peuvent franchir plusieurs stades de test, par exemple, des tests d'intégration puis d'assurance de la qualité ou des tests d'intégration et d'acceptation par l'utilisateur. Le cas échéant, les responsables installent les capacités de sécurité à chaque stade de test.

3.8.2 Effectuer les tests d'intégration de la sécurité

Objectifs :	Tester les aspects du système d'information liés à la sécurité en conformité avec les plans de tests de sécurité.
Rôle principal :	Testeur de systèmes
Rôles de soutien :	Praticien de la sécurité
Intrants :	(3.7.3-A) Représentation de la mise en œuvre du système d'information, incluant la sécurité (3.8.1-A) Environnement de test du système d'information, incluant la sécurité
Extrants :	(3.8.2-A) Plans, scénarios et résultats des tests d'intégration de la sécurité
Exigences relatives à l'assurance de la sécurité :	(3.6.1-C) Tâches techniques et exigences relatives au contenu des documents d'assurance de la sécurité pour les tests de sécurité (section 8, ST-E et ST-D) (3.6.1-C) Tâches techniques et exigences relatives au contenu des documents d'assurance de la sécurité pour l'évaluation des vulnérabilités (section 8, VA-E et VA-D)

Lignes directrices :

Les tests d'intégration de la sécurité de cette phase doivent être appliqués, tant sur le plan technique que sur le plan des procédures, à toutes les solutions de sécurité intégrées au système d'information, incluant les procédures de sécurité opérationnelles et les procédures d'installation des composants de sécurité. Ces tests incluent les tests de sécurité fonctionnels et peuvent également inclure les évaluations des vulnérabilités et les tests de pénétration, selon les exigences d'assurance de la sécurité. Les tests qui ont échoué doivent être examinés et, dans la mesure du possible, corrigés et effectués de nouveau au cours du cycle des tests de sécurité. La représentation de la mise en œuvre, les procédures de sécurité opérationnelles et les procédures d'installation des composants de sécurité doivent être mises à jour pour refléter tous les changements de nature corrective qui ont été apportés.

Au cours de cette activité, les intégrateurs de systèmes doivent produire des plans et des scénarios de tests de sécurité d'intégration, incluant les résultats prévus.

Nota : Les responsables des projets de TI doivent effectuer des tests de régression et communiquer leurs résultats, ainsi que les résultats des tests d'intégration de la sécurité, afin d'accroître la confiance à l'égard des changements et des mises à jour du système et confirmer qu'ils n'ont pas, par inadvertance, entraîné aucune faiblesse susceptible de poser des risques à la sécurité.

3.8.2.1 Évaluation des vulnérabilités et tests de pénétration

Selon les exigences d'assurance de la sécurité, les testeurs peuvent effectuer des évaluations des vulnérabilités pendant les tests d'intégration. À ce stade-ci, les objectifs des activités d'évaluation des vulnérabilités sont les suivants :

- S'assurer que les produits de TI installés ne présentent aucune vulnérabilité connue ou que les vulnérabilités connues sont documentées et ont été atténuées à un niveau acceptable;

- S'assurer que le renforcement de la sécurité (p. ex., la désactivation des ports et services TCP inutilisés) a été appliqué en conformité avec les normes et les meilleures pratiques du ministère et de l'industrie.

Il est possible que le testeur doive également effectuer des tests de pénétration pour valider certains aspects de la sécurité du système, par exemple, des tests pour évaluer la résilience d'une interface d'application Web à certaines attaques (p. ex., une injection SQL) ou celle du périmètre de sécurité du réseau, en appliquant des règles de pare-feu ou une configuration de renforcement de routeur.

3.8.3 Évaluer les tests d'intégration de la sécurité

Objectifs :	Confirmer que les tests de sécurité ont été effectués en conformité avec les exigences d'assurance de la sécurité.
Rôle principal :	Évaluateur de la sécurité
Rôles de soutien :	Praticien de la sécurité
Intrants :	(3.8.1-A) Environnement de test du système d'information, incluant la sécurité (3.8.2-A) Plans, scénarios et résultats des tests d'intégration de la sécurité
Extrants :	(3.8.3-A) Énoncé d'évaluation des tests d'intégration de la sécurité
Exigences relatives à l'assurance de la sécurité :	(3.6.1-C) Tâches d'évaluation d'assurance de la sécurité pour les tests de sécurité (section 8, ST-A) (3.6.1-C) Tâches d'évaluation d'assurance de la sécurité pour l'évaluation des vulnérabilités (section 8, VA-A)

Lignes directrices :

De pair avec le praticien de la sécurité, l'évaluateur de la sécurité doit effectuer les tâches suivantes :

- Confirmer que les travaux liés aux tests d'intégration de la sécurité respectent les tâches techniques et les exigences relatives au contenu des documents;
- Confirmer que les travaux liés à l'évaluation des vulnérabilités respectent les tâches techniques et les exigences relatives au contenu des documents;
- Préparer un énoncé d'évaluation aux fins d'approbation.

3.8.4 Approuver l'installation en production

Objectifs :	Obtenir l'autorisation de commencer l'installation du système d'information dans l'environnement de production en conformité avec la représentation de la mise en œuvre du système d'information.
Rôle principal :	Autorisateur
Rôles de soutien :	Évaluateur de la sécurité
Intrants :	(3.7.2-A) Énoncé d'évaluation de l'environnement de développement sécurisé (3.7.4-A) Énoncé d'évaluation du développement de la sécurité (3.8.3-A) Énoncé d'évaluation des tests d'intégration de la sécurité
Extrants :	(3.8.4-A) Autorisation de commencer la phase d'installation en production
Exigences relatives à l'assurance de la sécurité :	Aucune exigence particulière

Lignes directrices :

Cette activité est recommandée pour les grands projets de TI ou au moment de la mise en œuvre de systèmes qui appuient des programmes du GC ou des processus opérationnels plus critiques.

Le but principal de cette activité est d'obtenir de l'autorisateur l'approbation requise pour commencer l'installation du système d'information dans l'environnement de production, en conformité avec la représentation de la mise en œuvre. L'approbation peut être aussi simple qu'un compte rendu de décision d'un procès-verbal d'une réunion technique ou de projet, ou aussi formelle qu'une lettre d'approbation signée par l'autorisateur.

3.9 Phase d'installation

Cette sous-section décrit les activités du PASSI de la phase d'installation du CDS, qui font partie de la phase d'intégration et d'installation du CVS.

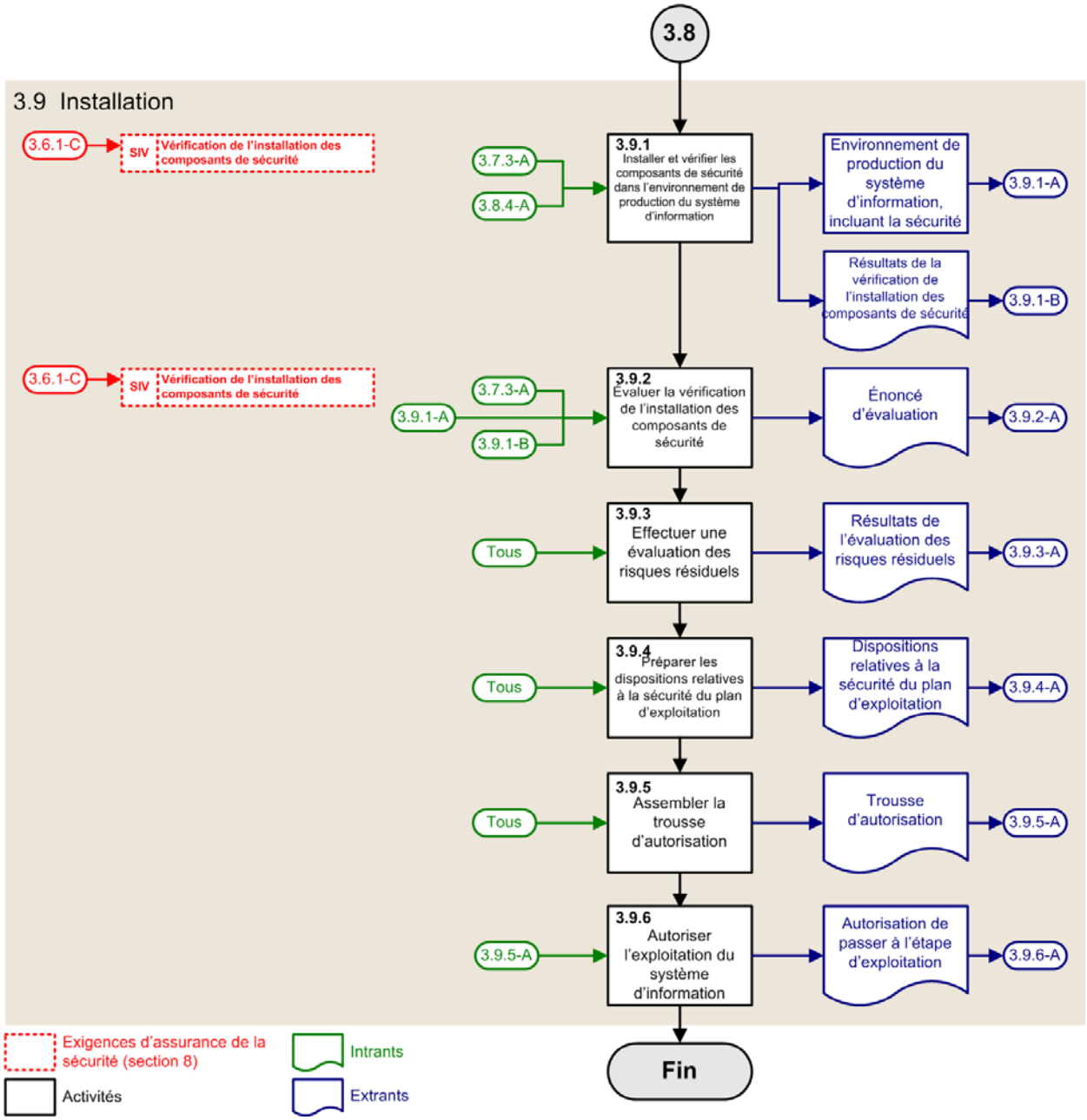


Figure 11 : Activités du PASSI – Phase d'installation

3.9.1 Installer et vérifier les composants de sécurité dans l'environnement de production du système d'information

Objectifs :	Installer les composants de sécurité dans l'environnement de production du système d'information et confirmer que l'installation et la configuration sont conformes à la représentation de la mise en œuvre.
Rôle principal :	Administrateur de système
Rôles de soutien :	Praticien de la sécurité
Intrants :	(3.7.3-A) Représentation de la mise en œuvre du système d'information, incluant la sécurité (3.8.4-A) Autorisation de commencer la phase d'installation en production
Extrants :	(3.9.1-A) Environnement de production du système d'information, incluant la sécurité (3.9.1-B) Résultats de la vérification de l'installation des composants de sécurité
Exigences relatives à l'assurance de la sécurité :	(3.6.1-C) Tâches techniques et exigences relatives au contenu des documents d'assurance de la sécurité pour la vérification de l'installation des composants de sécurité (section 8, SIV-E et SIV-D)

Lignes directrices :

Cette activité est exécutée en même temps que les activités d'installation du système d'information. Pendant le processus d'installation, le praticien de la sécurité vérifie l'installation des composants de sécurité comme le prescrivent les exigences d'assurance de la sécurité. Pour effectuer la vérification, il examine et inspecte les solutions de sécurité installées dans l'environnement de production afin de confirmer que tout est installé et configuré conformément à la représentation de la mise en œuvre. Tout écart relevé est corrigé au cours de cette activité.

3.9.2 Évaluer la vérification de l'installation des composants de sécurité

Objectifs :	Confirmer que la vérification de l'installation des composants de sécurité a été effectuée en conformité avec les exigences d'assurance de la sécurité.
Rôle principal :	Évaluateur de la sécurité
Rôles de soutien :	Praticien de la sécurité, administrateur de système
Intrants :	(3.7.3-A) Représentation de la mise en œuvre du système d'information, incluant la sécurité (3.9.1-A) Environnement de production du système d'information, incluant la sécurité (3.9.1-B) Résultats de la vérification de l'installation des composants de sécurité
Extrants :	(3.9.2-A) Énoncé d'évaluation de la vérification de l'installation des composants de sécurité
Exigences relatives à l'assurance de la sécurité :	(3.6.1-C) Tâches d'évaluation d'assurance de la sécurité pour la vérification de l'installation des composants de sécurité (section 8, SIV-A)

Lignes directrices :

De pair avec le praticien de la sécurité et l'administrateur de système, l'évaluateur de la sécurité doit exécuter les tâches suivantes :

- Confirmer que les travaux de vérification de l'installation des composants de sécurité correspondent aux tâches techniques et respectent les exigences relatives au contenu des documents;
- Préparer un énoncé d'évaluation aux fins d'approbation.

3.9.3 Effectuer une évaluation des risques résiduels

Objectifs :	Déterminer et documenter les niveaux de risque résiduel dans l'environnement d'exploitation du système d'information.
Rôle principal :	Évaluateur de la sécurité
Rôles de soutien :	Praticien de la sécurité
Intrants :	Tous les extrants précédents du PASSI
Extrants :	(3.9.3-A) Résultats de l'évaluation des risques résiduels
Exigences relatives à l'assurance de la sécurité :	Aucune exigence particulière

Lignes directrices :

Afin de mener à bien l'évaluation des risques résiduels, l'évaluateur, avec l'aide du praticien de la sécurité, devrait effectuer les tâches suivantes :

- Résumer les scénarios de risque ainsi que les décisions (c.-à-d. atténuer, éviter ou accepter) qui ont été documentés durant les activités d'EMR des phases de conception de haut niveau et de conception détaillée;
- Résumer les lacunes en matière de sécurité qui ont été cernées durant la phase de développement, la phase d'intégration et de test et la phase d'installation du CDS et qui n'ont pas été corrigées ni atténuées;
- Ajuster les niveaux de risque afin de déterminer le profil de risque en fonction duquel le système d'information sera exploité;
- Documenter les résultats dans un rapport d'évaluation des risques résiduels.

Il y a plusieurs raisons pour lesquelles des lacunes n'ont pas été corrigées à un stade si avancé du processus. Par exemple, les responsables du projet de TI peuvent avoir décidé de reporter à la phase de maintenance la correction d'un bogue mineur de module logiciel relevé durant les tests d'intégration de la sécurité afin d'éviter de retarder le projet au complet. Un autre exemple est celui d'un produit logiciel dans lequel une vulnérabilité a été relevée au cours d'une évaluation des vulnérabilités durant les tests d'intégration et pour lequel le fournisseur n'a pas été en mesure de produire de rustine ou de solution de rechange. L'activité d'évaluation des risques résiduels inclut une évaluation de l'incidence possible des lacunes non corrigées sur les risques et les vulnérabilités.

L'évaluateur devrait s'assurer que des demandes de changement ont été créées dans le système de gestion des changements pour chacune des lacunes en suspend. On ne recommande pas d'utiliser d'autres mécanismes comme un plan de mise en œuvre des mesures de protection.

En plus de l'évaluation et de la documentation des risques résiduels, cette activité peut également inclure la préparation d'un rapport d'EMR, le cas échéant. Les praticiens peuvent préparer un rapport d'EMR en regroupant les résultats des activités d'EMR, documentés durant les phases de conception de haut niveau (section 3.5.1.1) et détaillée (section 3.6.1.1), avec les résultats de l'évaluation des risques résiduels. De manière générale, la taille et la complexité d'un rapport d'EMR doivent correspondre à la taille et à la complexité du projet.

3.9.4 Préparer les dispositions relatives à la sécurité du plan d'exploitation

Objectifs :	Préparer les dispositions relatives à la sécurité du plan d'exploitation du système d'information.
Rôle principal :	Praticien de la sécurité
Rôles de soutien :	Évaluateur de la sécurité, personnel responsable des opérations de TI
Intrants :	Tous les extrants précédents du PASSI
Extrants :	(3.9.4-A) Dispositions relatives à la sécurité du plan d'exploitation
Exigences relatives à l'assurance de la sécurité :	Aucune exigence particulière

Lignes directrices :

Les dispositions relatives à la sécurité d'un plan d'exploitation établissent un calendrier de mesures et de procédures que le groupe opérationnel doit mettre en œuvre durant la phase d'exploitation et de maintenance pour s'assurer de maintenir la posture de sécurité du système et de gérer les risques de manière appropriée.

Les dispositions du plan d'exploitation incluent ce qui suit :

- Procédures de sécurité opérationnelles élaborées durant la phase de développement (section 3.7.3);
- Liste des lacunes de sécurité non réglées et plans et calendriers d'atténuation connexes.

3.9.5 Assembler la trousse d'autorisation

Objectifs :	Préparer une trousse d'autorisation, qui inclut les justifications nécessaires au soutien de l'autorisation de l'exploitation du système d'information.
Rôle principal :	Praticien de la sécurité
Rôles de soutien :	Évaluateur de la sécurité
Intrants :	Tous les extrants précédents du PASSI
Extrants :	(3.9.5-A) Trousse d'autorisation
Exigences relatives à l'assurance de la sécurité :	Aucune exigence particulière

Lignes directrices :

La trousse d'autorisation est présentée à l'autorisateur aux fins d'approbation. L'autorisateur et les gestionnaires de projet doivent convenir au début du projet de la composition exacte de la trousse

d'autorisation. Au minimum, la trousse doit inclure les énoncés d'évaluation, les résultats de l'évaluation des risques résiduels ou le rapport d'EMR, et le plan d'exploitation (qui inclut les dispositions relatives à la sécurité).

3.9.6 Autoriser l'exploitation du système d'information

Objectifs :	Autoriser l'exploitation du système d'information.
Rôle principal :	Autorisateur
Rôles de soutien :	Évaluateur de la sécurité, gestionnaire de projet
Intrants :	(3.9.5-A) Trousse d'autorisation
Extrants :	(3.9.6-A) Autorisation de passer à l'étape d'exploitation
Exigences relatives à l'assurance de la sécurité :	Aucune exigence particulière

Lignes directrices :

L'autorisateur est responsable d'autoriser l'exploitation du système d'information. La décision d'autoriser ou non l'exploitation est liée au contenu de la trousse d'autorisation. L'autorisateur peut émettre une autorisation de commencer, avec ou sans condition, ou un refus de procéder à cette étape. La décision relève de plusieurs facteurs, le plus important étant l'acceptabilité des risques résiduels et la nature des lacunes de sécurité non réglées.

Durant la phase d'exploitation et de maintenance du CVS, le système d'information est en état permanent d'autorisation. Cet état n'est pas une condition qui expire après une certaine période et qui doit être renouvelée. Une fois en production, le système fait l'objet d'une surveillance et d'une évaluation continues de la sécurité par le groupe responsable de la sécurité des TI ainsi que par la fonction de sécurité des TI, conformément aux lignes directrices énoncées à l'Annexe 1 du guide ITSG-33 [Référence 1]. Lorsque se produit un événement de sécurité majeur, l'autorisation de passer à l'étape d'exploitation peut être révoquée, ce qui équivaut essentiellement à priver le système de son statut opérationnel. Lorsqu'il se produit des événements de sécurité moins graves, ou en raison de résultats obtenus à l'issue d'une évaluation de la sécurité, l'autorisateur peut demander des mises à jour de la sécurité pour maintenir l'autorisation de passer à l'étape d'exploitation.

L'autorisation de passer à l'étape d'exploitation peut être transférée à l'individu ou à l'organisation qui a la responsabilité opérationnelle du système, tout comme aux intervenants, en présentant un énoncé formel d'autorisation. L'énoncé doit inclure la date de début de l'exploitation ainsi que toute condition en vertu de laquelle l'autorité a été accordée. Toute interdiction de passer à ce stade doit renvoyer à une étape du CDS où la cause profonde menant au refus peut être examinée à la satisfaction de l'autorisateur.

3.9.6.1 Plan de sécurité du système

En menant à terme les activités du PASSI, les responsables de projets de TI produisent les éléments d'information qui font normalement partie du plan de sécurité du système (qu'il ne faut pas confondre avec

le plan de sécurité ministérielle, discuté à l'Annexe 1 du guide ITSG-33 [Référence 1]). Bien que le PASSI prône la minimisation de toute documentation de sécurité indépendante en favorisant l'intégration de ses extrants aux produits livrables de projet habituels, il n'interdit pas l'utilisation de plans de sécurité de système. Lorsque les ministères ont déjà établi le besoin de plans de sécurité de système dans leur profil de contrôle de sécurité ou les profils de domaine, les responsables de projets de TI peuvent facilement en préparer un pour leur système en regroupant les éléments d'information des différents extrants du PASSI. Le contrôle de sécurité PL-2 à l'Annexe 3 du guide ITSG-33 [Référence 7] renferme plus de détails.

4 Phase d'exploitation et de maintenance sécurisées

Cette section inclut, à l'intention des ministères, des lignes directrices générales concernant les activités de sécurité qui contribuent à maintenir la posture de sécurité des systèmes d'information durant leur période de production.

Bien que le PASSI soit, à strictement parler, une méthodologie liée au CDS, certaines activités liées à la sécurité, menées par les groupes responsables des opérations, font partie d'un processus de CVS élargi qui vise à préserver la posture de sécurité des systèmes mis en place dans le cadre de projets de TI. Ces activités sont liées au maintien de la sécurité durant la phase d'exploitation et de maintenance d'un processus de CVS type.

4.1 Maintenir l'exploitation sécurisée

Objectifs :	Maintenir la posture de sécurité du système d'information durant la phase d'exploitation et de maintenance du CVS en assurant l'administration et la maintenance des solutions de sécurité mises en œuvre.
Rôle principal :	Personnel responsable des opérations de TI, administrateur de système
Rôles de soutien :	Concepteur de systèmes, développeur de systèmes, intégrateur de systèmes, coordonnateur de la sécurité des TI, praticien de la sécurité, évaluateur (externe) de la sécurité
Intrants :	(3.7.3-A) Représentation de la mise en œuvre du système d'information, incluant la sécurité (3.9.4-A) Dispositions relatives à la sécurité du plan d'exploitation
Extrants :	(4.1-A) Extrants produits durant l'exploitation sécurisée du système d'information, p. ex., documents de gestion du changement et des problèmes, rapports sur les incidents, mises à jour de la configuration de la sécurité, journaux système globaux (qui incluent les documents sur les événements système et sur les événements liés à la sécurité, à la vérification, aux applications, à la détection d'intrusions, etc.) et paramètres de rendement de la solution de sécurité. (4.1-B) Représentation à jour de la mise en œuvre du système d'information
Exigences relatives à l'assurance de la sécurité :	Exigences variées selon l'activité (p. ex., la mise en œuvre d'un changement apporté à la conception peut nécessiter des activités d'ingénierie, de documentation et de test).

Lignes directrices :

Les groupes responsables des opérations de TI administrent et assurent la sécurité du système durant la phase d'exploitation et de maintenance du CVS, conformément aux dispositions relatives à la sécurité du plan d'exploitation (tel que défini à la section 3.9.4). Le processus d'administration et de maintenance permet de s'assurer que les solutions de sécurité sont configurées et utilisées de manière appropriée.

Pour assurer de manière efficace la maintenance et l'administration de la sécurité des systèmes, les ministères :

- établissent et attribuent les rôles et les responsabilités liés à la sécurité opérationnelle;
- assurent la sensibilisation et la formation en matière de sécurité du personnel opérationnel et des utilisateurs;
- appliquent aux solutions de sécurité des tâches périodiques de maintenance et d'administration de la sécurité;
- analysent, déterminent et mettent en œuvre les changements apportés aux solutions de sécurité afin de tenir compte des nouvelles exigences, de l'évolution des menaces, des incidents de sécurité et du signalement de nouvelles vulnérabilités;
- appliquent les rustines et les mises à jour de sécurité;
- gèrent les configurations de sécurité.

Durant la phase opérationnelle, les groupes responsables des opérations de TI protègent la posture de sécurité des systèmes en suivant les processus et procédures prévus en cas de problèmes de sécurité, lesquels sont documentés dans les plans de gestion du changement et de la configuration. Les changements apportés au cours de cette période peuvent nécessiter des modifications aux solutions de sécurité ou avoir une incidence sur la posture de sécurité du système. Toute demande de changement doit décrire l'incidence qu'aura ou que pourrait avoir le changement sur la sécurité. Lorsque l'on croit que les changements sont susceptibles d'accroître les risques résiduels, les groupes responsables des opérations de TI doivent déterminer, par des activités d'EMR, s'il y a lieu de prévoir des contrôles et des solutions de sécurité supplémentaires ou des changements en nombre supérieur à ceux prévus, pour maintenir les risques résiduels à des niveaux acceptables. Dans le cas de changements majeurs, les groupes doivent, suivant les conseils des autorisateurs, demander l'aide d'évaluateurs de la sécurité pour effectuer les évaluations d'incidences. L'autorisateur, avec l'aide du groupe responsable des opérations de TI, des praticiens et des évaluateurs de la sécurité, peut décider que certains changements sont assez importants pour justifier le lancement d'un nouveau projet de TI. Ce type de projet doit se conformer au PASSI imposé par le ministère.

Pour gérer les changements de manière sécuritaire, les ministères doivent tenir compte des lignes directrices suivantes :

Pour les mises à niveau habituelles ou les changements apportés aux systèmes d'information :

- Inclure les évaluations d'incidences dans un processus formel de demande de changement;
- Demander aux autorités opérationnelles d'approuver la demande.

Pour les changements majeurs apportés aux systèmes d'information :

- Inclure les évaluations d'incidences dans un processus formel de demande de changement;
- Demander aux autorités opérationnelles et aux autorisateurs d'approuver la demande;
- Au choix, demander à un évaluateur de la sécurité d'effectuer une analyse.

De plus, afin de respecter le processus d'autorisation (voir la section 5.5 de l'Annexe 1 du guide ITSG-33 [Référence 1]), les ministères doivent au moins exiger que les activités de sécurité suivantes soient menées au moment d'effectuer les mises à niveau et les changements :

- Effectuer des tests de sécurité et communiquer les résultats au moment du déploiement de nouveaux composants système;
- Effectuer une évaluation des vulnérabilités pour s'assurer de maintenir la posture de sécurité du système d'information;
- Mettre à jour les évaluations de risque résiduel du système d'information ou les rapports d'EMR pour saisir les résultats des évaluations d'incidences.

4.2 Surveiller et évaluer la sécurité

Objectifs :	Surveiller et évaluer en permanence le rendement des solutions de sécurité mises en œuvre durant la phase d'exploitation et de maintenance du CVS pour s'assurer que le système d'information répond de manière uniforme à ses objectifs de sécurité.
Rôle principal :	Surveillance : personnel responsable des opérations de TI, praticiens de la sécurité (s'il existe une fonction de Centre de protection de l'information [CPI]) Évaluation : Praticien de la sécurité, évaluateur (externe) de la sécurité
Rôles de soutien :	Coordonnateur de la sécurité des TI
Intrants :	Rapports des organismes-conseils du GC Rapports d'évaluation des menaces et des vulnérabilités de sources ouvertes (4.1-A) Extrants produits durant l'exploitation sécurisée (4.1-B) Représentation à jour de la mise en œuvre du système d'information
Extrants :	(4.2-A) Extrants de la surveillance et de l'évaluation de la sécurité, p. ex., tableau de bord de la gestion des risques liés à la sécurité des TI, rapports sur les incidents de sécurité, rapports de l'EMR, rapports d'évaluation des vulnérabilités, rapports sur les tests de pénétration, rapports sur le rendement de la sécurité, rapports du CPI.
Exigences relatives à l'assurance de la sécurité :	Les exigences énoncées à la section 3 s'appliquent aux activités effectuées (p. ex., les exigences VA-E et VA-D décrites à la section 8.4.12 s'appliqueraient à une évaluation des vulnérabilités).

Lignes directrices :

Les groupes responsables des opérations de TI doivent surveiller et évaluer en permanence la posture de sécurité de leurs systèmes en collaboration avec la fonction de sécurité des TI et un CPI[7] ministériel, le cas échéant. La surveillance et l'évaluation continues de la sécurité sont des processus essentiels qui aident les

[7] La responsabilité de la surveillance et de l'évaluation permanentes de la sécurité peut être partagée entre le groupe responsable du ministère et un CPI, ou prise entièrement en charge par le CPI du ministère.

ministères à effectuer leurs activités de détection et d'intervention en temps opportun en cas d'attaques, de brèches de sécurité et d'autres événements et changements potentiellement compromettants à l'intérieur ou à l'extérieur de l'environnement du système d'information. Ces activités permanentes informent la fonction de sécurité des TI qu'il convient d'entreprendre des changements de nature corrective dans le cadre de processus de gestion des incidents, de gestion du changement et d'autres processus.

Pour assurer la surveillance de la posture de sécurité de leurs systèmes de manière efficace, les groupes responsables des opérations de TI, en collaboration avec les praticiens de la fonction de sécurité des TI ou un CPI, doivent effectuer les activités suivantes :

- Surveiller et analyser les changements liés aux menaces, aux vulnérabilités, aux incidences et aux risques, et déterminer s'il faut apporter des changements;
- Surveiller le rendement et l'efficacité fonctionnelle des mécanismes de sécurité et des solutions;
- Analyser les documents liés aux événements afin de déterminer la cause des événements de sécurité;
- Cerner et signaler les incidents de sécurité et intervenir;
- Protéger de manière adéquate les journaux, les rapports et d'autres artefacts de surveillance de la sécurité.

Les groupes responsables des opérations de TI, en collaboration avec la fonction ministérielle de sécurité des TI, doivent cerner de manière appropriée les incidents de sécurité et coordonner adéquatement les processus et procédures d'intervention, de reprise et de production de rapports afin d'éviter ou de limiter les incidences, de permettre la reprise des opérations et d'informer les responsables du ministère. Dans certains cas, les activités d'intervention et de reprise peuvent nécessiter un effort coordonné d'autres groupes tant de l'intérieur que de l'extérieur du ministère.

Pour appuyer les activités de gestion des risques liés à la sécurité des TI, les responsables des activités de surveillance et d'évaluation continues de la sécurité doivent informer les cadres supérieurs du rendement global de la posture de sécurité des TI du ministère. Ces communications permettent de déterminer les occasions d'amélioration et d'apporter des changements au niveau de la fonction de sécurité des TI. Voir l'Annexe 1 du guide ITSG-33 [Référence 1] pour plus de détails sur les activités de surveillance et d'évaluation de la sécurité des TI du ministère.

4.3 Maintenir l'autorisation

Objectifs :	Maintenir l'autorisation du système d'information durant la phase d'exploitation et de maintenance du CVS.
Rôle principal :	Autorisateur
Rôles de soutien :	Évaluateur (externe) de la sécurité, praticiens de la sécurité
Intrants :	(4.1-A) Extrants produits durant l'exploitation sécurisée (4.1-B) Représentation à jour de la mise en œuvre du système d'information (4.2-A) Extrants de la surveillance et de l'évaluation de la sécurité
Extrants :	Instructions et recommandations de l'autorisateur
Exigences relatives à l'assurance de la sécurité :	Aucune exigence particulière.

Lignes directrices :

Cette activité est menée de pair avec l'activité de maintien de l'autorité au niveau du ministère. Voir l'Annexe 1 du guide ITSG-33 [Référence 1] pour plus de détails sur ces activités et sur les autres activités de gestion des risques liés à la sécurité des TI. Il est important que les groupes responsables des opérations de TI conservent des dossiers à jour sur leurs activités de maintenance, d'administration, de surveillance et d'évaluation de la sécurité et documentent de manière adéquate les changements, les incidents et toutes les mesures correctives liés à la sécurité dans l'environnement du système d'information. Une bonne documentation opérationnelle de la sécurité simplifie le maintien des mécanismes d'autorisation.

5 Phase d'élimination

Cette section inclut, à l'intention des ministères, des lignes directrices concernant l'élimination sécurisée des biens de TI lorsqu'un système d'information atteint la fin de sa vie utile.

5.1 Élimination sécurisée des biens de TI

Objectifs :	Éliminer les biens de TI en toute sécurité.
Rôle principal :	Praticien de la sécurité, administrateur de système
Rôles de soutien :	Évaluateur de la sécurité
Intrants :	Demande formelle d'élimination du système d'information, incluant un plan d'élimination Documents de gestion de la configuration et des biens du système d'information (3.9.4-A) Dispositions relatives à la sécurité du plan d'exploitation
Extrants :	(5.1-A) Rapport d'élimination
Exigences relatives à l'assurance de la sécurité :	Aucune exigence particulière

Lignes directrices :

Lorsqu'un système d'information atteint la fin de sa vie utile et doit être retiré de l'environnement de production, le groupe responsable des opérations de TI doit éliminer les biens de TI sensibles en conformité avec les procédures d'élimination sécurisée du plan d'exploitation (voir la section 3.9.4). Les processus et les procédures de soutien de cette fonction incluent ce qui suit :

- Nettoyage des supports;
- Élimination sécurisée des supports;
- Gestion de la configuration et des biens;
- Procédures de sécurité spéciales telle l'élimination de dispositifs cryptographiques contrôlés ou d'équipement TEMPEST.

Les groupes responsables des opérations de TI doivent produire un rapport d'élimination qui indique clairement les biens de TI éliminés, la méthode utilisée et l'autorité responsable de l'élimination. Cette procédure est particulièrement importante pour les supports de TI, les dispositifs cryptographiques contrôlés et l'équipement TEMPEST. Le rapport d'élimination doit également indiquer les fichiers de données supprimés, déplacés et archivés.

5.2 Évaluer les résultats de l'élimination

Objectifs :	Confirmer que les activités d'élimination ont été menées en conformité avec les exigences de la section 5.1.
Rôle principal :	Évaluateur (externe) de la sécurité
Rôles de soutien :	Praticien de la sécurité, administrateur de système
Intrants :	(5.1-A) Rapport d'élimination
Extrants :	(5.2-A) Énoncé d'évaluation des activités d'élimination
Exigences relatives à l'assurance de la sécurité :	Aucune exigence particulière

Lignes directrices :

Les évaluateurs de la sécurité doivent examiner le rapport d'élimination du système d'information pour confirmer que les biens de TI sensibles ont été éliminés complètement et de manière sécurisée, en conformité avec les dispositions du plan d'exploitation et toutes autres politiques et normes applicables, et présenter un énoncé d'évaluation à l'autorisateur du système d'information. Avant de diffuser l'énoncé, les évaluateurs doivent s'assurer de corriger rapidement, et à la satisfaction de l'autorisateur, toute lacune relevée au cours des activités d'élimination.

5.3 Approbation définitive

Objectifs :	Documenter l'autorisation des activités d'élimination et du retrait du système d'information.
Rôle principal :	Autorisateur
Rôles de soutien :	Évaluateur (externe) de la sécurité
Intrants :	(5.2-A) Énoncé d'évaluation des activités d'élimination
Extrants :	(5.3-A) Approbation définitive
Exigences relatives à l'assurance de la sécurité :	Aucune exigence particulière

Lignes directrices :

Après avoir examiné l'énoncé d'évaluation des activités d'élimination, les autorisateurs doivent confirmer leur approbation de la mise hors service du système d'information. L'approbation définitive doit être transmise à la fonction de sécurité des TI aux fins d'archivage. Les autorisateurs doivent également en informer les propriétaires des activités opérationnelles soutenues par le système d'information, par exemple, en leur transmettant une copie de l'approbation définitive.

6 Capacités externes

Les responsables d'un projet de TI intègrent à leur système une capacité externe lorsqu'ils prévoient tirer avantage d'une capacité offerte par un système d'information différent de celui qui sera mis en place à la fin du projet. Dans ce cas, le fournisseur de la capacité peut être une autre organisation du ministère parrain, un autre ministère ou un fournisseur de services commercial. La décision de recourir à une capacité externe peut être imposée par le SCT ou le ministère parrain, ou peut être le résultat d'une analyse des besoins ou de la conception. Quelle que soit la raison, les responsables des projets de TI doivent déterminer l'ensemble des exigences de sécurité auxquelles la capacité et son fournisseur doivent répondre et utiliser cet ensemble comme base pour acquérir la capacité.

Les responsables qui intègrent une capacité externe suivent les étapes du PASSI décrites dans les sections précédentes et doivent prévoir une activité supplémentaire, soit la spécification des exigences de sécurité propres à la capacité externe. Ces exigences sont liées à plusieurs facteurs, notamment : les exigences d'assurance de la sécurité, les besoins opérationnels en matière de sécurité et les contrôles de sécurité de système associés à la capacité externe, et le niveau d'influence qu'exerce le projet de TI ou le ministère parrain sur la posture de sécurité du système d'information utilisé par le fournisseur. Les exigences de sécurité peuvent porter sur les fonctions de sécurité (p. ex., authentification forte de l'utilisateur final), la sécurité des systèmes d'information du fournisseur (p. ex., forte capacité interne de gestion des incidents), ou la confiance que l'on peut avoir en la capacité du fournisseur de livrer son produit de manière sécurisée.

La Figure 12 illustre, dans le contexte du CDS, l'activité du PASSI qui permet de spécifier les exigences de sécurité d'une capacité externe. Les intrants de cette activité peuvent inclure :

- Les exigences d'assurance de la sécurité de la phase de conception;
- Les besoins opérationnels en matière de sécurité et les contrôles de sécurité de système de la phase d'analyse des besoins;
- Les autres exigences de sécurité potentiellement requises aux fins de la politique ou de la gestion des risques;
- Les spécifications de conception de la sécurité de la phase de conception de haut niveau.

Une fois définies, ces exigences servent d'intrants au processus d'approvisionnement pour l'acquisition de la capacité externe du fournisseur. Le type de processus varie selon que le fournisseur est à l'intérieur du ministère (p. ex., négociation d'un protocole d'entente [PE]), un autre ministère (p. ex., négociation d'une entente formelle sur les niveaux de service [ENS]), ou un fournisseur de services privé (p. ex., présentation d'une DP). Dans tous les cas, le processus inclut une évaluation qui permet de s'assurer que la capacité externe répond à toutes les exigences de sécurité applicables.

L'ensemble exact des activités du PASSI varie selon la manière dont la capacité externe sera utilisée. Si elle doit être intégrée à un système d'information existant, les travaux de conception détaillée, de développement et d'intégration et de test seront limités aux seuls nouveaux composants ou interfaces nécessaires à l'utilisation de la capacité. Si la capacité est utilisée comme service autonome, les activités prendront probablement fin lorsque le processus d'approvisionnement sera terminé.

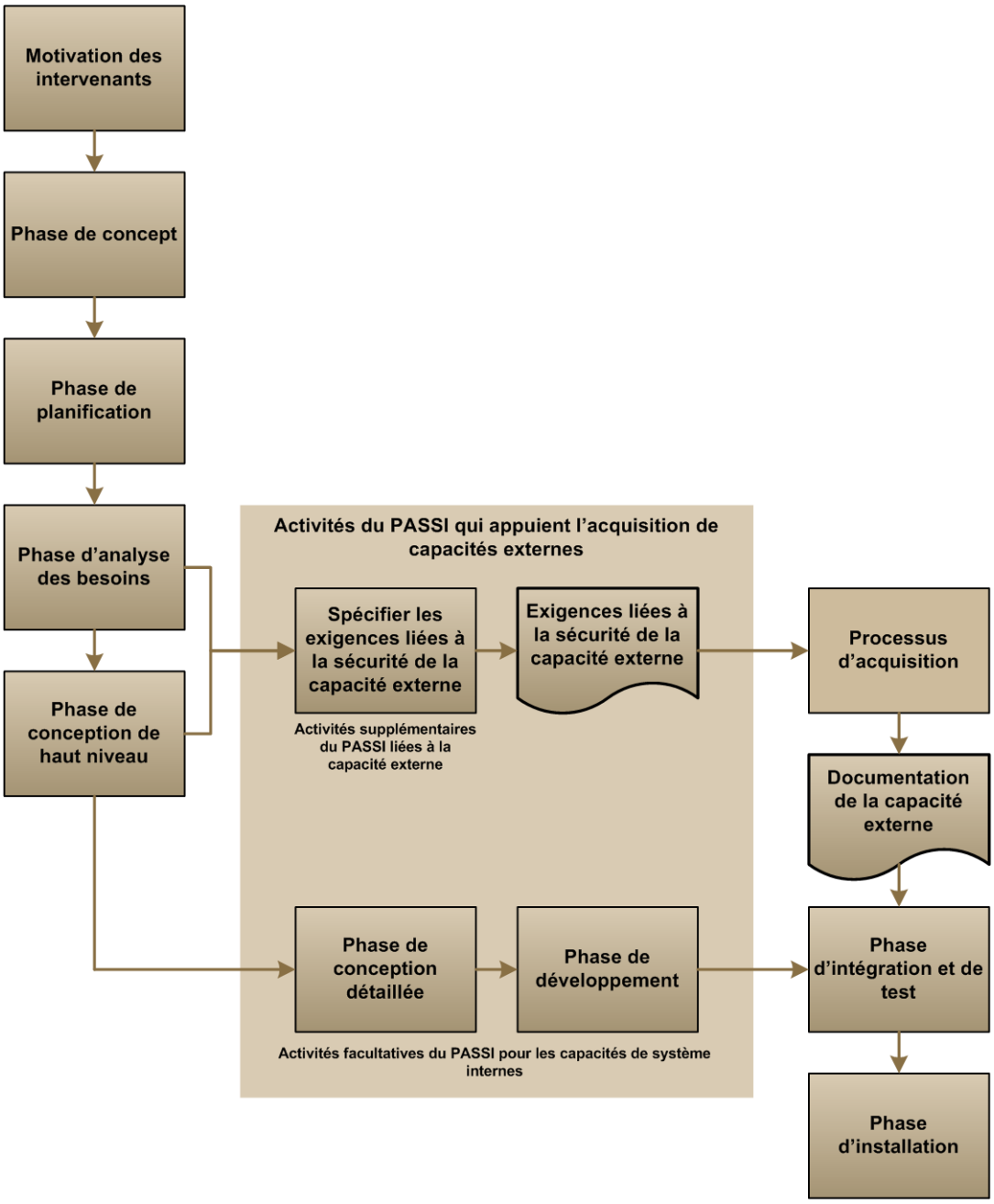


Figure 12 : PASSI incluant les activités liées aux capacités externes

Les ministères peuvent également envisager de recourir à la certification ISO 27001 [Référence 9] comme moyen d'évaluer la maturité des fournisseurs de services privés en matière de sécurité des TI lorsqu'ils acquièrent des capacités externes. Toutefois, cette certification seule ne garantit pas que la posture de sécurité déclarée de la capacité externe d'un fournisseur privé réponde aux besoins. Les ministères doivent

donc évaluer la certification revendiquée par le fournisseur et la conformité aux autres exigences de sécurité durant le processus d'évaluation des soumissions.

6.1 Utiliser des services de TI autorisés

Les ministères qui sont tenus d'utiliser un service de TI autorisé doivent favoriser une approche légèrement différente de celle décrite précédemment. Ils doivent évaluer la posture de sécurité que les services de TI du fournisseur adoptent pour soutenir leurs propres activités opérationnelles afin (1) de déterminer les contrôles de sécurité supplémentaires qui devront être mis en place dans leur environnement ou (2) de comprendre les risques auxquels les ministères eux-mêmes s'exposent.

Pour réussir une telle évaluation, les ministères doivent pouvoir compter sur un programme de gestion des risques liés à la sécurité qui inclut les éléments suivants :

- Une fonction établie de gestion des risques liés à la sécurité des TI qui répond aux exigences de la PSG [Référence 3] et de la DGMS [Référence 4] (p. ex., une fonction basée sur l'Annexe 1 du guide ITSG-33 [Référence 1], sur la norme ISO 27001 [Référence 9] ou sur la publication 800-39 du NIST [Référence 13]) et qui fonctionne à un niveau de maturité conforme à la sensibilité et la criticité de leurs programmes;
- Un processus établi d'application de la sécurité dans les systèmes d'information (c.-à-d., un CDS sécurisé ou un processus d'ingénierie de sécurité de système) qui convient aux besoins de l'organisme;
- Une évaluation ministérielle des menaces qui documente les menaces jugées pertinentes à la portée du document et une justification des menaces jugées non pertinentes ou non applicables;
- Un ou plusieurs profils de contrôle de sécurité ministérielle qui documentent les contrôles de base des systèmes d'information qui soutiennent les activités opérationnelles du ministère. Chaque profil doit documenter les hypothèses relatives au contexte opérationnel, au contexte de menace et au contexte technique, ainsi que les approches de sécurité applicables. Il doit également inclure le niveau acceptable de risque résiduel que les systèmes associés au profil peuvent tolérer;
- Une capacité de surveillance continue qui permet d'analyser la posture de sécurité des systèmes d'information internes et externes (p. ex., ceux des autres ministères du GC ou des fournisseurs de services de TI privés). Cette capacité doit inclure des indicateurs clés de rendement de la sécurité et des paramètres de mesure échec-réussite. L'analyse de la posture de sécurité inclut, par exemple, les résultats des activités suivantes :
    - Évaluations périodiques de la sécurité (p. ex., évaluation de l'infrastructure de sauvegarde de réseau et des pratiques connexes, vérification de la configuration d'un service de détection de maliciels, analyse des vulnérabilités d'un service d'authentification commun);
    - Examens périodiques des rapports sur les incidents (p. ex., un serveur compromis a laissé exfiltrer des données, le serveur a été nettoyé et reconstruit sur des bases sécurisées, les vulnérabilités ont été corrigées et une fonction de surveillance supplémentaire a été mise en place);
    - Examens périodiques des événements liés à la sécurité (p. ex., des données journalisées indiquent un nombre inhabituel de tentatives infructueuses de connexion à une base de données);

- Évaluations périodiques des activités liées à la sécurité effectuées par le personnel opérationnel (p. ex., des administrateurs qui utilisent leurs comptes privilégiés exclusivement pour des tâches administratives et non pour naviguer sur le Web).

Une fois ces éléments clés en place, les ministères sont en mesure d'évaluer un service de TI autorisé pour autant qu'ils aient accès aux renseignements suivants :

- Description détaillée de la fonction de gestion des risques du fournisseur. Par exemple :
  - La fonction de gestion du fournisseur n'est pas documentée;
  - La fonction de gestion du fournisseur est documentée, mais n'est pas exécutée de manière uniforme;
  - Le processus de gestion du fournisseur est documenté et certifié par un vérificateur externe (p. ex., certification ISO 27001).
- Description détaillée du processus d'application de la sécurité dans les systèmes d'information utilisés par le fournisseur. Par exemple :
  - Le processus du fournisseur n'est pas documenté;
  - Le processus du fournisseur est documenté, mais n'est pas exécuté de manière uniforme;
  - Le processus du fournisseur est documenté et ce dernier est en mesure de prouver qu'il l'applique de manière rigoureuse durant la mise en œuvre du service de TI autorisé.
- Évaluation détaillée des menaces par le fournisseur. Par exemple :
  - Le processus d'évaluation des menaces du fournisseur n'est pas documenté;
  - Le processus d'évaluation des menaces du fournisseur est documenté, mais n'a pas été utilisé au maximum durant l'établissement de la fonction de gestion des risques et la mise en œuvre du service de TI autorisé;
  - Le processus d'évaluation des menaces du fournisseur est documenté et ce dernier est en mesure de prouver qu'il l'a utilisé au maximum durant l'établissement de la fonction de gestion des risques et la mise en œuvre du service de TI autorisé.
- Le fournisseur utilise un ou plusieurs profils de contrôle de sécurité. Par exemple :
  - Le profil de contrôle de sécurité (ou une spécification d'exigences de sécurité équivalentes) du fournisseur n'est pas documenté;
  - Le profil de contrôle de sécurité du fournisseur est documenté, mais n'a été appliqué que partiellement durant l'établissement de la fonction de gestion des risques et la mise en œuvre du service de TI autorisé;
  - Le profil de contrôle de sécurité du fournisseur est documenté et ce dernier est en mesure de prouver qu'il l'a appliqué au maximum durant l'établissement de la fonction de gestion des risques et la mise en œuvre du service de TI autorisé. Tous les contrôles de sécurité qui ne sont pas actuellement appliqués sont documentés; une justification est fournie ainsi qu'un plan de mise en œuvre, le cas échéant.

- Renseignements de sécurité détaillés requis pour effectuer une analyse de la posture de sécurité du service de TI autorisé. Par exemple :
    - Des rapports d'évaluation des contrôles de sécurité du service de TI autorisé sont produits périodiquement et sur demande (p. ex., après un incident);
    - Les rapports sont produits rapidement pour tous les incidents concernés;
    - Les rapports sont produits rapidement pour tous les événements liés à la sécurité;
    - Des rapports d'évaluation des activités liées à la sécurité menées par le personnel opérationnel sont produits périodiquement et sur demande (p. ex., après un incident ou un changement majeur apporté à l'infrastructure du fournisseur).

Les ministères peuvent évaluer la mesure dans laquelle la posture de sécurité d'un service de TI est adéquate en comparant les éléments clés de sa fonction de gestion des risques liés à la sécurité des TI (c.-à-d. processus de gestion des risques, processus d'application de la sécurité dans les systèmes d'information, évaluation des menaces, profils de contrôle de sécurité et capacité analytique et de surveillance, qui comprend les indicateurs de rendement et les paramètres clés de la sécurité) à l'information liée à la sécurité mentionnée ci-dessus.

Si les éléments clés et les renseignements de sécurité fournis correspondent et se comparent favorablement, les ministères peuvent conclure que la posture de sécurité du service de TI lui permet de prendre en charge les activités opérationnelles au niveau acceptable de risque résiduel documenté.

Si la fonction de sécurité des TI du ministère n'a pas produit ces éléments clés ou ne les a produits que partiellement, l'évaluation ne peut être effectuée de façon irréfutable. Cette affirmation vaut également pour tout fournisseur qui ne peut produire les renseignements requis ou lorsque les renseignements sont inadéquats. Dans ce cas, on ne peut tirer aucune conclusion définitive quant à la pertinence de la posture de sécurité du service de TI relativement à la prise en charge des activités opérationnelles.

7 Déterminer le niveau de robustesse

7.1 Introduction

Au cours des activités du PASSI, le praticien de la sécurité doit déterminer le niveau de robustesse requis des différents contrôles de sécurité. Cette section définit le concept de robustesse, décrit un modèle de robustesse[8] et propose une méthodologie qui permet de déterminer un niveau approprié de robustesse pour un contrôle de sécurité (ou un ensemble de contrôles de sécurité). Cette méthodologie offre aux praticiens une façon uniforme de concevoir et d'appliquer des solutions de sécurité appropriées pour protéger les systèmes d'information.

7.2 Robustesse

La robustesse permet de caractériser la *force* et l'*assurance* de la sécurité d'un contrôle de sécurité. La force de la sécurité est associée à la capacité potentielle du contrôle de protéger la confidentialité, l'intégrité ou la disponibilité des biens de TI. L'assurance de la sécurité d'un contrôle est liée à la confiance en la conception et la mise en œuvre adéquates du contrôle et à sa capacité de fonctionner de la manière prévue. Ensemble, ces deux caractéristiques définissent les exigences que la mise en œuvre d'un contrôle doit respecter pour satisfaire à son objectif de sécurité. Par exemple, un contrôle conceptuellement fort (p. ex., un algorithme de chiffrement AES [Advanced Encryption Standard]) qui n'offre aucune assurance (c.-à-d. aucune preuve ne démontre que l'algorithme est codé correctement) aura un niveau de robustesse plus faible qu'un contrôle similaire qui offre un niveau d'assurance supérieur (p. ex., un logiciel qui a été validé).

Les contrôles utilisés pour protéger des biens de TI plus sensibles ou essentiels ou qui sont exposés à des menaces plus sérieuses exigent normalement des solutions de sécurité plus fortes et une mise en œuvre offrant une meilleure assurance et requièrent donc des niveaux de robustesse plus élevés. Le modèle de robustesse définit une hiérarchie de niveaux de robustesse basés sur les niveaux de préjudice prévus et sur les capacités ou l'ampleur des menaces.

7.3 Composants du modèle de robustesse

Le Tableau 4 définit un modèle basé sur cinq niveaux de robustesse (R1 à R5) et leurs exigences en matière de force et d'assurance. Ces niveaux ont été adaptés pour contrer un ensemble défini de catégories de menace (présentées à la section 7.4.2).

Les cinq niveaux définis dans ce modèle ne s'appliquent pas nécessairement à tous les contrôles (p. ex., la mise en œuvre de certains contrôles, tels ceux pour la sauvegarde ou la vérification, peut ne pas exiger une robustesse de niveau 4 ou 5). Les exigences relatives à la force de la sécurité sont propres à chaque contrôle. Celles de l'assurance de la sécurité sont généralement les mêmes pour tous les contrôles qui exigent un même niveau de robustesse.

[8] Le modèle de robustesse du CST est basé sur une approche développée par la National Security Agency (NSA) et documentée à la section 4 (Technical Security Countermeasures) du document *Information Assurance Technical Framework* (IATF) [Référence 10].

Tableau 4 : Définitions des niveaux de robustesse

Robustesse		Force de la sécurité	Assurance de la sécurité	
			Niveau	Description
Faible	**R1**	Force de base. Pour les menaces délibérées; résiste aux menaces non sophistiquées (comparables à celles des catégories Md1 à Md3); toutefois, il est attendu que des attaques plus sophistiquées réussiront à compromettre les biens de TI protégés.	NAS 1	Exige un faible niveau d'assurance de la sécurité.
	R2	Pour les menaces liées aux risques accidentels ou naturels; résiste aux événements de menace des catégories Ma1 et Ma2; toutefois, il est attendu que des événements de menace plus graves compromettront les biens de TI protégés.	NAS 2	Exige un niveau moyen d'assurance de la sécurité.
Moyenne	**R3**	Force moyenne. Pour les menaces délibérées; résiste aux menaces sophistiquées (comparables à celles des catégories Md4 et Md5); toutefois, il est attendu que certaines attaques sophistiquées réussiront à compromettre les biens de TI protégés. Ces contrôles peuvent normalement contrer une menace résultant d'un effort conjugué (p. ex., un groupe de pirates organisé). Pour les menaces liées aux risques accidentels ou naturels; résiste aux événements de menace des catégories Ma3 et Ma4; toutefois, il est attendu que les événements de menace très graves compromettront les biens de TI protégés.	NAS 3	Exige le meilleur niveau d'assurance de la sécurité offert dans le commerce; les développeurs ou les utilisateurs sont prêts à assumer des coûts de conception de sécurité supplémentaires.
Élevée	**R4**	Force élevée ou niveau supérieur. Pour les menaces délibérées; résiste aux menaces les plus sophistiquées (comparables à celles des catégories Md6 et Md7); il ne devrait y avoir raisonnablement aucun moyen que des attaques réussissent à compromettre les biens de TI. Elle peut résister à des menaces d'un laboratoire national ou d'un État-nation.	NAS 4	*Actuellement hors de la portée de ce guide*
	R5	Pour les menaces liées aux risques accidentels ou naturels; résiste aux événements de menace de la catégorie Ma5; est seulement vulnérable aux événements de menace de proportions catastrophiques.	NAS 5	*Actuellement hors de la portée de ce guide*

Chaque niveau de robustesse du Tableau 4 est associé à une des trois principales catégories : faible, moyenne et élevée. De plus, chaque niveau de robustesse individuel, R1 à R5, est formé de deux composants : force de la sécurité et assurance de la sécurité.

- **Force de la sécurité** – Caractérisation du potentiel[9] qu'offre un contrôle existant relativement à la protection de la confidentialité, de l'intégrité et de la disponibilité des biens de TI contre les capacités des agents de menace, les risques naturels ou les événements accidentels. Les efforts (coûts) ou l'ampleur de la menace que l'agent doit déployer pour contourner le contrôle en place croissent avec l'augmentation de la force de la sécurité.
- **Assurance de la sécurité** – Tâches de renforcement de la confiance qui visent à s'assurer qu'un contrôle de sécurité est conçu et appliqué correctement et qu'il fonctionne tel que prévu. De plus, l'assurance de la sécurité comprend des tâches dont le but est de confirmer la capacité de tous les contrôles d'un système d'information (conception, mise en œuvre et exploitation) à répondre aux besoins opérationnels en matière de sécurité.

Chacun des aspects de la robustesse est décrit en détail dans les sous-sections suivantes.

7.3.1 Niveau de la force de la sécurité

La force de la sécurité d'un contrôle à un niveau de robustesse donné est liée aux critères spécifiques de la conception et aux mécanismes d'application du contrôle. Comme il est indiqué dans le Tableau 4, la force varie d'un niveau de base à un niveau élevé, et chaque niveau vise à contrer une ou plusieurs catégories de capacité de menace. Ces capacités (M1 à M7) sont définies à la section 7.4.2 et incluent les menaces délibérées et accidentelles.

Pour appliquer un contrôle de sécurité (p. ex., authentification, autorisation), on utilise un ou plusieurs mécanismes de sécurité (p. ex., mot de passe à usage unique, listes de contrôle d'accès). La force d'un contrôle et des mécanismes qui servent à l'appliquer est liée aux critères de conception utilisés pour contrer les capacités des agents de menace identifiées et leurs méthodes d'attaque, ou les risques naturels et les événements accidentels identifiés. Remarquez que la force est une mesure relative des efforts (coûts) ou de l'ampleur de la menace nécessaires pour contourner ou compromettre le contrôle et n'est liée d'aucune façon à son coût de mise en œuvre.

Le but du modèle de robustesse est de s'assurer que les contrôles dotés d'une force de même niveau offrent une protection comparable, soit contrer des menaces équivalentes. Toutefois, sélectionner le même niveau de force pour tous les contrôles ne garantit pas que l'ensemble du système et ses mécanismes de sécurité offriront ce même niveau de protection. Une analyse globale de l'ingénierie de sécurité du système doit être effectuée pour évaluer la force réelle de l'ensemble de la solution.

Les critères de conception nécessaires à la mise en œuvre d'un contrôle à un niveau de force donné sont énoncés dans des publications spécialisées tel le guide ITSG-31 – *Guide sur l'authentification des utilisateurs pour les systèmes TI* [Référence 8]. Le site Web du CST (www.cse-cst.gc.ca/its-sti/publications/index-fra.html) donne une liste des publications actuelles.

[9] Il convient de noter que le potentiel de protection d'un contrôle de sécurité peut se matérialiser uniquement lorsque la mise en œuvre du contrôle est effectuée à un niveau d'assurance de la sécurité adéquat.

7.3.2 Niveau d'assurance de la sécurité

L'assurance de la sécurité d'un contrôle (ou d'un ensemble de contrôles) à un niveau de robustesse donné est définie par un ensemble de tâches qui doivent être exécutées durant la mise en œuvre et qui confirmeront que le ou les contrôles répondent aux objectifs prévus.

Chaque niveau de robustesse inclut un composant d'assurance de la sécurité désigné par un niveau d'assurance de la sécurité (NAS) spécifique, qui peut varier d'un niveau faible (NAS1) à un niveau très élevé (NAS5). Les niveaux d'assurance définis dans le présent document sont les suivants :

- **NAS1** – Exige un faible niveau d'assurance de la sécurité;
- **NAS2** – Exige un niveau moyen d'assurance de la sécurité;
- **NAS3** – Exige le meilleur niveau d'assurance de la sécurité offert dans le commerce; les développeurs ou les utilisateurs sont prêts à assumer des coûts de conception de sécurité supplémentaires.

Les niveaux NAS4 et NAS5[10] sont actuellement hors de la portée du présent guide. La section 8 définit plus en détail les niveaux d'assurance de la sécurité.

La mise en place de l'assurance de la sécurité est le résultat des tâches effectuées par les développeurs, les réalisateurs et les évaluateurs de la sécurité du système. Les efforts supplémentaires qui touchent ou un plusieurs des éléments suivants permettent d'accroître cette assurance :

- **Meilleures pratiques de conception** – Utilisation de la conception modulaire, définition claire des interfaces, jumelage lâche des fonctions et autres pratiques de conception qui améliorent la qualité de la conception. Une plus grande maturité du processus de développement permet l'utilisation de meilleures pratiques de conception[11];
- **Meilleure documentation** – Documentation de conception complète, précise et bien gérée qui améliore la qualité de la mise en œuvre des systèmes et réduit les probabilités d'erreurs et d'omissions;
- **Portée** – Élargissement de la portée des efforts de conception et d'évaluation (p. ex., inclure les détails des sous-systèmes plutôt que de simples interfaces augmente l'assurance globale du système);
- **Profondeur** – Les efforts de conception et d'évaluation sont plus rentables puisqu'ils sont déployés à un plus grand niveau de détail;
- **Rigueur** – Les efforts de conception et d'évaluation sont plus rentables puisqu'ils sont déployés de manière plus formelle et structurée.

Ces tâches peuvent, par exemple, permettre de confirmer que les besoins opérationnels en matière de sécurité sont justifiés, que l'ensemble sélectionné de contrôles de sécurité répond à ces besoins et que les contrôles sont conçus et appliqués correctement et fonctionnent comme prévu. L'objectif est de consacrer les efforts nécessaires pour obtenir le niveau requis d'assurance de la sécurité.

[10] Communiquer avec les Services à la clientèle de la Sécurité des TI du CSTC pour obtenir des conseils liés aux niveaux d'assurance NAS4 et NAS5.

[11] Par exemple, voir les sites *Software Engineering Institute - Capability Maturity Model Integration*, www.sei.cmu.edu et *System Security Engineering – Capability Maturity Model*, www.sse-cmm.org.

7.3.2.1 Confiance à l'égard des fournisseurs et développeurs

En plus des éléments d'assurance de la sécurité mentionnés précédemment, il est essentiel de pouvoir se fier aux fournisseurs qui offrent des conceptions, des produits et des solutions de sécurité. L'accroissement des niveaux de préjudice, des catégories de capacités des agents de menace et de l'ampleur des événements de menace (et, donc, du niveau de robustesse requis) fait en sorte que l'on doit également augmenter la confiance à l'égard des fournisseurs.

Les ministères peuvent établir la confiance à l'égard des fournisseurs en partie grâce au processus d'appel d'offres du GC en remplissant une liste de vérification des exigences relatives à la sécurité (LVERS) fournie avec les documents de demande de soumissions. Cette liste permet aux ministères de formuler une exigence qui impose au fournisseur de se conformer aux exigences du Programme de sécurité industrielle. Ce programme est géré par TPSGC.

Par l'entremise de ce programme, TPSGC peut accorder soit une vérification d'organisation désignée aux niveaux cotés Protégé A, B ou C, soit une attestation de sécurité d'installation aux niveaux Confidentiel, Secret, Très secret, OTAN Confidentiel ou OTAN Secret. Selon le niveau de sécurité recherché, le processus peut inclure une évaluation qui permet d'établir que l'organisation n'est pas soumise à une influence étrangère; la nomination officielle (suivie d'une enquête de sécurité) d'un responsable de la sécurité de l'entreprise; des enquêtes de sécurité sur les cadres supérieurs clés, les employés et les sous-traitants; une évaluation de la sécurité matérielle, etc. Ce programme établit la confiance en la loyauté et l'intégrité avec lesquelles une entreprise et ses employés offrent leurs services au gouvernement du Canada et constitue donc un élément de confiance important.

Pour les niveaux d'assurance NAS1 à NAS3, le fournisseur doit détenir, au minimum, une vérification d'organisation désignée. Pour les niveaux NAS4 et NAS5, il doit détenir une attestation de sécurité d'installation. Le niveau de vérification ou d'autorisation doit être déterminé par une EMR et tenir compte du rôle spécifique du fournisseur et des connaissances qu'il acquerra relativement au système d'information. Aux fins d'uniformité, on recommande aux ministères d'établir une norme organisationnelle à cet effet. De manière générale, les travaux de développement qui nécessitent des niveaux d'assurance plus élevés (NAS4 et supérieurs) doivent exiger des fournisseurs qu'ils détiennent au minimum une attestation de sécurité d'installation de niveau Secret.

7.4 Déterminer un niveau de robustesse rentable

7.4.1 Déterminer les niveaux de préjudice

La première étape de l'établissement d'un niveau de robustesse rentable pour un contrôle de sécurité consiste à déterminer les niveaux de préjudice associés aux biens de TI que le contrôle doit protéger. Comme il est expliqué à la section 3.5.1.2, les niveaux de préjudice des objectifs de sécurité (confidentialité, intégrité et disponibilité) sont tributaires de la catégorie de sécurité des activités opérationnelles prises en charge par les biens de TI.

Plusieurs contrôles de sécurité protègent les biens de TI contre la compromission de deux ou trois de ces objectifs de sécurité simultanément (p. ex., le contrôle d'accès). Dans la plupart des cas, pour déterminer la robustesse, on recommande d'utiliser le plus élevé des trois niveaux de préjudice. Par exemple, à un bien de TI qui assure le soutien d'une activité opérationnelle associée aux niveaux de préjudice cotés Protégé B, intégrité élevée et disponibilité faible, on attribuera un niveau de préjudice élevé.

Pour la sélection du niveau de robustesse, les niveaux de préjudice sont désignés de P1 (très faible) à P5 (très élevé).

7.4.2 Déterminer la catégorie de capacités des agents de menace et l'ampleur de l'événement

La deuxième étape de l'établissement d'un niveau de robustesse rentable consiste à sélectionner une catégorie de menace délibérée pertinente dans le Tableau 5, et l'ampleur correspondante de la menace accidentelle ou du risque naturel dans le Tableau 6. L'intrant de ce processus est le rapport d'évaluation des menaces, normalement validé au début de la phase de concept du CDS (voir la section 3.2.1).

Les catégories de menace définies dans ces tableaux représentent un niveau croissant des capacités des agents de menace et de l'ampleur des menaces accidentelles et des risques naturels. Au fur et à mesure de l'évolution des capacités des agents de menace, les exemples dans le tableau correspondant seront mis à jour. Puisque ce tableau contient uniquement des exemples, les évaluations ministérielles des menaces doivent documenter l'information actuelle sur les capacités des agents de menace qui concernent l'organisme.

Tableau 5 : Descriptions et exemples de catégories de menace délibérée

Catégorie de menace	Agent de menace	Exemples de capacités croissantes des agents de menace
Md1	Attaquant non malveillant (p. ex., navigation, modification ou destruction d'information interdites non malveillantes dues à un manque de formation, de sensibilisation ou d'attention)	• Capacités de base de l'utilisateur d'accéder aux systèmes d'information et au contenu.
Md2	Attaquant occasionnel et passif possédant un minimum de ressources et disposé à prendre de petits risques (p. ex., écoute clandestine, pirates ados).	• Exécution d'un scanneur de vulnérabilité accessible au public • Exécution de scripts d'attaque de serveurs • Tentatives de suppression aléatoire de fichiers système • Modification des paramètres de fichiers de configuration
Md3	Attaquant possédant un minimum de ressources et disposé à prendre des risques importants (p. ex., pirates peu sophistiqués).	• Utilisation d'outils de piratage accessibles au public pour effectuer différents exploits • Employés qui installent des chevaux de Troie et des enregistreurs de frappe dans les systèmes non protégés • Utilisation d'attaques par hameçonnage simples pour compromettre les cibles avec du maliciel • Exécution de programmes dans le but de faire planter les ordinateurs et les applications
Md4	Attaquant sophistiqué possédant des ressources moyennes et disposé à prendre de petits risques (p. ex., crime organisé, pirates sophistiqués, organisations internationales).	• Utilisation experte d'outils de piratage accessibles au public, incluant les attaques du jour zéro • Capacité de créer ses propres outils d'attaque dans le logiciel • Attaques par ingénierie sociale de base • Capacité d'assemblage de matériel avec des composants grand public pour faciliter les attaques • Attaques par hameçonnage pour accéder aux cartes de crédit ou aux renseignements personnels
Md5	Attaquant sophistiqué possédant des ressources moyennes et disposé à prendre de grands risques (p. ex., crime organisé, terroristes internationaux).	• Corruption d'employés internes pour obtenir de l'information • Modification de produits commerciaux ou utilisation de produits frauduleux en vue d'un gain financier (p. ex., trafiquage d'un guichet automatique ou guichet falsifié) • Destruction physique de l'infrastructure • Attaques par canal auxiliaire (p. ex., cartes à puce)

Catégorie de menace	Agent de menace	Exemples de capacités croissantes des agents de menace
Md6	Attaquant extrêmement sophistiqué possédant des ressources abondantes et disposé à prendre de petits risques (p. ex., laboratoires nationaux bien financés, États-nations, organisations internationales).	• Attaques de type TEMPEST • Attaques de la chaîne d'approvisionnement, tel le trafiquage de produits commerciaux ou l'utilisation de produits frauduleux en vue d'activités d'espionnage (p. ex., pare-feu ou routeurs de réseau falsifiés) • Technologies d'implantation difficiles à détecter dans le matériel ou le logiciel • Exploitation de vulnérabilités non publiques
Md7	Attaquant extrêmement sophistiqué possédant des ressources abondantes et disposé à prendre des risques extrêmes (p. ex., États-nations en période de crise).	• Corruption, chantage ou intimidation d'employés internes en vue de compromettre la sécurité des systèmes • Pénétration dans des installations sécurisées en vue de permettre des attaques

Tableau 6 : Descriptions des catégories de menace accidentelle et de risque naturel

Catégorie de menace	Ampleur des événements
Ma1	• Événements accidentels mineurs (p. ex., trébucher sur un câble d'alimentation, entrer des données erronées)
Ma2	• Événements accidentels moyens (p. ex., rendre un serveur inutilisable, corrompre une base de données, divulguer de l'information à une mauvaise personne ou organisation) • Pannes matérielles ou logicielles mineures (p. ex., panne de disque dur) • Pannes mécaniques mineures (p. ex., panne de courant dans une section d'une installation) • Risques naturels mineurs (p. ex., inondation locale ou tremblement de terre qui compromettent une partie d'une installation)
Ma3	• Événements involontaires ou accidentels graves (p. ex., sectionnement des câbles de télécommunications ou d'alimentation d'une installation, incendie dans l'installation, compromission d'information à grande échelle) • Pannes mécaniques moyennes (p. ex., panne de courant prolongée dans une installation) • Risques naturels moyens (p. ex., inondation locale ou tremblement de terre qui compromettent une installation)
Ma4	• Pannes mécaniques graves (p. ex., panne de courant prolongée à l'échelle de la ville) • Risques naturels graves (p. ex., tremblement de terre avec dévastation à l'échelle de la ville)
Ma5	• Pannes mécaniques très graves (p. ex., panne de courant prolongée à l'échelle régionale) • Risques naturels très graves (p. ex., tremblement de terre avec dévastation à l'échelle régionale ou nationale)

7.4.3 Déterminer le niveau de robustesse

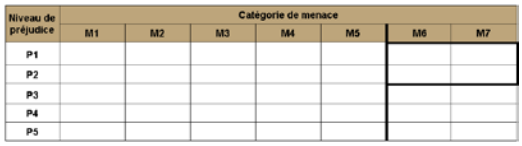
Pour déterminer un niveau de robustesse rentable pour un contrôle de sécurité (ou un ensemble de contrôles ayant des exigences similaires), les praticiens de la sécurité choisissent dans le Tableau 7 le niveau de robustesse correspondant au niveau de préjudice évalué (de P1 à P5) et la catégorie de menace (de M1 à M7) associée à un ou à plusieurs contrôles de sécurité. Les niveaux de robustesse recommandés visent à atténuer les capacités des agents de menace (menaces délibérées) et l'ampleur des événements (menaces accidentelles et risques naturels) précisées pour obtenir des risques résiduels ***faibles*** pour les objectifs de sécurité (confidentialité, intégrité et disponibilité).

Tableau 7 : Niveau de robustesse rentable recommandé pour obtenir des risques résiduels faibles

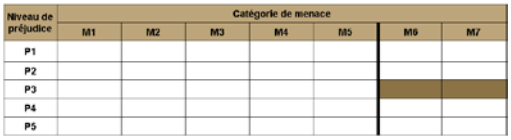
Niveau de préjudice	Catégorie de menace						
	M1	**M2**	**M3**	**M4**	**M5**	**M6**	**M7**
P1	R1	R1	R1	R2	R2	*R4*	*R4*
P2	R1	R1	R1	R2	R2	*R4*	*R4*
P3	R1	R1	R2	R3	R3	R4	R4
P4	*R1*	*R2*	*R3*	*R3*	*R3*	R4	R5
P5	*R1*	*R2*	*R3*	*R3*	R4	R5	R5

7.4.3.1 Description et explication du tableau

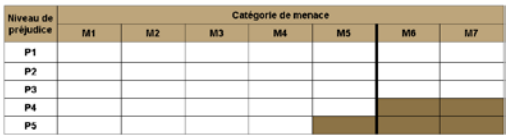
Les cellules ombrées brun pâle du Tableau 7 (P1-M1 à P3-M5) représentent des scénarios types de biens de TI protégés qui appuient des activités opérationnelles d'une catégorie de sécurité associée à des niveaux de préjudice de très faibles à moyens (c.-à-d. cotés Confidentiel, Protégé B et niveaux inférieurs, et intégrité ou disponibilité de moyenne à faible), dont la catégorie de menace est évaluée à un niveau de faible à élevé. Les niveaux de robustesse recommandés varient de R1 à R3, niveaux normalement associés à des solutions de sécurité de produits commerciaux de bas de gamme à haut de gamme.



Les cellules blanches dont le texte est en italique (P1-M6 à P2-M7) représentent des scénarios de biens de TI protégés qui appuient des activités opérationnelles d'une catégorie de sécurité associée à des niveaux de préjudice de très faibles à faibles (c.-à-d. non classifiés et cotés Protégé A, et intégrité ou disponibilité de très faible à faible), dont la catégorie de menace est évaluée à un niveau très élevé. Le niveau de robustesse minimal requis pour atténuer des menaces extrêmement sophistiquées (p. ex., les services de renseignement étranger d'un État-nation) est R4, niveau normalement associé à des solutions de sécurité gouvernementales standards de gamme moyenne à haute. Toutefois, dans ce cas précis, le coût de la solution est généralement jugé prohibitif compte tenu du niveau de sensibilité faible des biens de TI à protéger et l'on opte normalement pour un niveau de robustesse plus faible (p. ex., R2). Il est alors impossible de contrer les menaces extrêmement sophistiquées et les risques courus sont formellement acceptés.



Les cellules ombrées foncées (P3-M6 et P3-M7) représentent des scénarios de biens de TI protégés qui appuient des activités opérationnelles d'une catégorie de sécurité associée à un niveau de préjudice moyen normalement lié au traitement de renseignements confidentiels, dont la catégorie de menace est évaluée à un niveau très élevé. Le niveau de robustesse recommandé est R4, niveau normalement associé à des solutions de sécurité gouvernementales standards de gamme moyenne à haute. Dans le cas des renseignements confidentiels, on recommande le niveau R4 aux fins d'harmonisation avec les traités d'alliance avec les partenaires étrangers et l'OTAN. On recommande que les systèmes qui traitent de l'information classifiée et qui ont été déployés en vue d'une utilisation par l'armée ou l'OTAN soient construits de manière à atténuer les menaces de la catégorie M7.



Les cellules ombrées foncées (P4-M6, P4-M7, P5-M5 à P5-M7) représentent des scénarios de biens de TI protégés qui appuient des activités opérationnelles d'une catégorie de sécurité associée à des niveaux de préjudice élevés à très élevés (c.-à-d. cotés Protégé C, Secret et Très secret, et intégrité ou disponibilité élevée à très élevée), dont la catégorie de menace est évaluée à un niveau élevé à très élevé. Les niveaux de robustesse recommandés varient de R4 à R5, niveaux normalement associés à des solutions de sécurité gouvernementales standards haut de gamme, incluant les solutions qui utilisent des dispositifs cryptographiques de type 1. Pour ces niveaux élevés de préjudice et de catégorie de menace, il n'est pas recommandé, pour atténuer les risques,

de recourir uniquement à des contrôles dont le niveau de robustesse est faible. N'oubliez pas que les politiques COMSEC du CST s'appliquent lorsqu'il s'agit de protéger de l'information classifiée.

Les cellules blanches dont le texte est en italique (P4-M1 à P5-M4) représentent des scénarios types de biens de TI protégés qui appuient des activités opérationnelles d'une catégorie de sécurité de niveau de préjudice élevé (c.-à-d. coté Protégé C, Secret et Très secret, et intégrité ou disponibilité élevée à très élevée), dont la catégorie de menace est évaluée à un niveau de faible à moyen. Exemple de ce type de scénario : la menace interne que représente un environnement à niveau dominant de sécurité physiquement séparé et dédié[12], et protégé par des mécanismes de sécurité matérielle adéquats, pour lesquels les utilisateurs possèdent une cote de sécurité appropriée et qui ne sont pas branchés à des systèmes dont le niveau de classification est inférieur (incluant Internet). Il est important, au moment de sélectionner ces niveaux de robustesse pour les contrôles de sécurité internes, de veiller à ce que la catégorie de menace évaluée soit vraiment d'un niveau faible à moyen (p. ex., capacités de menace de base à capacités de menace sophistiquées, excluant explicitement les capacités extrêmement sophistiquées). Toute menace interne connue, tout environnement opérationnel inhabituel (p. ex., une ambassade canadienne en pays hostile) ou toute frontière poreuse (p. ex., des ports USB non contrôlés) aura une influence importante sur la catégorie de menace évaluée.

La cellule (P4-M5) représente un scénario de biens de TI protégés qui appuient des activités opérationnelles d'une catégorie de sécurité de niveau de préjudice élevé (c.-à-d., coté Protégé C, Secret, à intégrité ou disponibilité élevée), dont la catégorie de menace est évaluée à un niveau de menaces sophistiquées. Ce scénario peut inclure des systèmes d'information d'organismes antiterroristes ou chargés de l'application de la loi qui traitent des renseignements qui doivent être protégés contre les menaces émanant du crime organisé. Les menaces extrêmement sophistiquées imputables aux États-nations sont jugées hors de la portée de ce guide puisque cette information est déjà partagée entre plusieurs organismes internationaux. Dans ce cas, on doit envisager d'utiliser des solutions de sécurité commerciales haut de gamme ou gouvernementales standards bas de gamme.

Le Tableau 8 inclut des exemples de systèmes d'information types et une évaluation du niveau de robustesse requis pour les principaux contrôles de sécurité de ces systèmes (le niveau de robustesse de certains contrôles peut être inférieur selon la conception de la sécurité. Voir l'exemple dans le texte explicatif des cellules P4-M1 à P5-M4 du Tableau 7). Puisque les exemples du Tableau 8 sont utilisés à des fins d'illustration, on ne tient compte que des menaces délibérées.

[12] Un environnement dédié à niveau dominant de sécurité est un système de TI pour lequel tous les utilisateurs possèdent une autorisation d'accès formelle et un besoin de connaître, et à qui on a attribué une cote de sécurité correspondant à la plus haute classification des données traitées ou stockées.

Tableau 8 : Exemples simples de détermination des niveaux de robustesse des contrôles de sécurité (seules les menaces délibérées sont prises en compte)

Exemple de système d'information	Description	Contrôles de sécurité clés Niveau de robustesse	
		Détermination	Niveau
Serveur wiki non classifié dans une zone restreinte ministérielle	• Traite des pages wiki non classifiées ayant des exigences faibles sur le plan de l'intégrité et de la disponibilité. • Serveur non connecté ou accessible à tout réseau externe ou public, incluant Internet.	Évaluation du niveau de préjudice prévu : très faible (P1). Évaluation de l'environnement de menace : très faible (Md1).	R1
Réseau ministériel du GC	• Réseau ministériel du GC qui contient des applications administratives et collaboratives de faible sensibilité et quelques applications personnalisées. • Les fonctionnaires ont accès à Internet.	Évaluation du niveau de préjudice prévu : faible (P2). Évaluation de l'environnement de menace : moyen (Md4).	R2
Application Web axée sur les transactions (non essentielle)	Application Web utilisée par une vaste collectivité d'utilisateurs et qui offre des services du GC en ligne (p. ex., une banque d'emplois dans laquelle des candidats éventuels peuvent verser ou mettre à jour leur curriculum vitæ).	Évaluation du niveau de préjudice prévu : faible (P2). Évaluation de l'environnement de menace : moyen (Md4).	
Application Web axée sur les transactions (essentielle à la mission)	Application Web utilisée par une vaste collectivité d'utilisateurs et qui offre des services du GC en ligne (p. ex., des transactions financières ou liées à la santé).	Évaluation du niveau de préjudice prévu : moyen (P3). Évaluation de l'environnement de menace : moyen (Md4 à Md5).	R3
Application collaborative pour le partage d'information secrète entre les organismes chargés de l'application de la loi	• Application collaborative (courrier électronique, affichage sur tableau blanc, messagerie instantanée, etc.) utilisée par le personnel chargé de l'application de la loi pour échanger de l'information secrète. • L'application collaborative fonctionne à l'intérieur de frontières protégées.	Évaluation du niveau de préjudice prévu : élevé (P4). Évaluation de l'environnement de menace : moyen (Md5).	
Système de contrôle de centrale nucléaire	• Le système contrôle tous les aspects du processus de production de la centrale. • Le système de contrôle n'est pas connecté directement à des réseaux externes; toutefois, les utilisateurs ont accès à des ordinateurs connectés à Internet dans la salle de contrôle.	Évaluation du niveau de préjudice prévu : très élevé (P5). Évaluation de l'environnement de menace : moyen (Md5).	R4

Exemple de système d'information	Description	Contrôles de sécurité clés Niveau de robustesse	
		Détermination	Niveau
Transfert de renseignements entre des domaines cotés Très secret et Protégé	Solution interdomaine utilisée pour transférer des données entre un domaine coté Très secret et un domaine coté Protégé.	Évaluation du niveau de préjudice prévu : très élevé (P5). Évaluation de l'environnement de menace : élevé (Md6).	R5
Transfert de renseignements militaires cotés Très secret	Transfert par liaison satellitaire de renseignements militaires cotés Très secret entre une base située en territoire hostile et l'administration centrale à Ottawa.	Évaluation du niveau de préjudice prévu : très élevé (P5). Évaluation de l'environnement de menace : élevé (Md7).	

7.5 Non-respect des exigences en matière de robustesse

Au cours de l'application d'un contrôle de sécurité, il est possible que les responsables d'un projet de TI optent pour un niveau de robustesse inférieur au niveau requis ou ne se conforment pas à certaines exigences recommandées en matière de robustesse. Cela aura pour effet de réduire l'efficacité avec laquelle le contrôle atténue des menaces particulières. Les raisons peuvent inclure, sans s'y limiter, un coût prohibitif, un manque de solution commerciale disponible offrant les fonctions appropriées ou une urgence opérationnelle. La justification d'une telle décision doit être documentée dans les activités d'EMR et permettra un réexamen du choix de niveau de robustesse lorsque les circonstances changeront.

8 Exigences d'assurance de la sécurité

8.1 Introduction

Cette section définit les exigences en matière d'assurance de la sécurité pour les projets de TI. Les exigences sont groupées en 13 sujets, selon leurs objectifs. Un niveau d'assurance de la sécurité (NAS) consiste en un ensemble présélectionné d'exigences d'assurance qui permettent un niveau croissant de confiance en la pertinence de l'ingénierie de sécurité et des travaux de documentation effectués par l'équipe de projet et, ultimement, en la capacité des contrôles appliqués à fonctionner comme prévu et à répondre aux besoins opérationnels en matière de sécurité. Cette section définit les niveaux actuels 1 à 3 d'assurance de la sécurité. Les définitions des niveaux 4 et 5 sont actuellement hors de la portée du présent guide[13].

Chaque exigence d'assurance de la sécurité comprend des tâches techniques, des exigences relatives au contenu des documents, et des tâches d'évaluation à effectuer dans le cadre du projet. Dans le contexte de l'assurance de la sécurité, une tâche technique est une activité liée un aspect technique de la sécurité (p. ex., la sélection et la documentation des contrôles de sécurité de système dans les spécifications de contrôle de sécurité). Une exigence relative au contenu des documents précise la structure et le contenu des produits, ou extrants, d'une tâche technique (p. ex., le niveau de détail de la description des contrôles dans une spécification de contrôle de sécurité). Une tâche d'évaluation est une activité qui permet de déterminer si une tâche technique et ses extrants répondent aux exigences d'assurance de la sécurité (p. ex., vérifier si les contrôles sont en fait décrits suffisamment en détail dans une spécification de contrôle de sécurité).

Une tâche d'évaluation inclut toutes les étapes que l'évaluateur de la sécurité doit franchir pour s'assurer que les responsables de projet corrigent les lacunes d'exécution des tâches techniques et de leur documentation, ainsi que les étapes nécessaires pour confirmer que les mesures correctives ont été prises. Cette activité vise essentiellement à faire en sorte que le processus de correction des lacunes fasse partie intégrante de chaque tâche d'évaluation. En respectant ces pratiques, les responsables peuvent corriger les problèmes liés à l'assurance de la sécurité dès qu'ils sont cernés par l'évaluateur de la sécurité et, ainsi, s'assurer d'atteindre les cibles d'assurance de la sécurité à la fin de chaque phase.

Les autorités de projet peuvent décider à n'importe quel moment de ne pas donner suite à une recommandation de l'évaluateur. Par exemple, l'autorisateur peut déterminer que le coût d'une recommandation, qui vise la mise en œuvre d'un contrôle supplémentaire pour mieux atténuer une menace particulière, est prohibitif et décider plutôt d'accepter le risque. Les évaluateurs doivent s'assurer que les énoncés d'évaluation tiennent compte de telles décisions et de toute incidence qu'elles peuvent avoir sur les risques résiduels.

La rigueur des exigences d'assurance de la sécurité varie en fonction de l'augmentation du niveau d'assurance. Cette rigueur est liée aux efforts consacrés à l'exécution de la tâche. Par exemple, une exigence peut imposer de documenter de manière formelle les contrôles de sécurité, et une autre, plus rigoureuse techniquement, d'inclure dans la spécification la raison pour laquelle chaque contrôle répond aux besoins opérationnels qui lui sont associés (c.-à-d. produire une justification du contrôle de sécurité).

[13] Communiquer avec les Services à la clientèle de la Sécurité des TI du CSTC pour obtenir des conseils liés aux niveaux d'assurance NAS4 et NAS5.

Les 13 types d'exigences d'assurance de la sécurité et leurs objectifs sont les suivants :

- **Besoins opérationnels en matière de sécurité** – Établir que les besoins opérationnels en matière de sécurité pour le système d'information ont été correctement définis;
- **Spécification des contrôles de sécurité** – Établir que les contrôles de sécurité ont été correctement définis et répondent aux besoins opérationnels qui leur sont associés;
- **Spécifications de conception** – Établir que la conception de la sécurité associée à la conception du système d'information respecte tous les contrôles de sécurité;
- **Évaluation des menaces et des risques** – Établir que la conception de la sécurité du système d'information atténue les menaces de manière adéquate;
- **Gestion du changement durant le développement** – Établir que la gestion des éléments du système d'information (p. ex., le code source de l'application) durant le développement est effectuée de manière adéquate;
- **Mesures de sécurité liées à l'environnement de développement** – Établir que la sécurité de l'environnement de développement est adéquate (p. ex., protection contre les modifications non autorisées du code source);
- **Outils de développement** – Établir que la sélection et l'utilisation des outils de développement appropriés sont adéquates (p. ex., outils de développement commerciaux ou de source ouverte, s'assurer que seuls des outils autorisés sont utilisés);
- **Pratiques de développement sécurisées** – Établir que le système d'information a été développé en suivant des pratiques sécurisées (p. ex., utilisation d'outils et de techniques d'analyse du code source, examen du code source, pratiques de programmation robustes);
- **Tests de sécurité** – Établir que les solutions de sécurité respectent les exigences de conception, ont été mises en œuvre correctement et fonctionnent comme prévu;
- **Procédures de sécurité opérationnelles** – Établir que les procédures sécurisées d'utilisation, d'administration et de maintenance du système d'information seront effectuées de manière adéquate durant la période d'exploitation du système;
- **Procédures d'installation des composants de sécurité** – Établir que le système d'information peut être installé de manière sécurisée dans l'environnement de production;
- **Évaluation des vulnérabilités** – Établir que le système d'information ne présente aucune vulnérabilité ou que les vulnérabilités ont été atténuées à un niveau acceptable de risque résiduel;
- **Vérification de l'installation des composants de sécurité** – Établir que les composants de sécurité du système d'information ont été installés et configurés correctement dans l'environnement de production.

8.2 Utilisation

Le Tableau 9 indique l'ensemble proposé d'exigences d'assurance de la sécurité que l'on peut utiliser durant un projet de TI, selon l'analyse effectuée durant la phase de conception du projet. Cet ensemble

peut être mieux ciblé durant les phases de conception détaillée et de haut niveau afin de tenir compte des exigences particulières de la conception de la sécurité.

8.3 Définitions des niveaux d'assurance de la sécurité

Durant la phase de concept du PASSI, les gestionnaires de projets de TI et les praticiens de la sécurité précisent le niveau d'effort approprié requis (associé à la robustesse requise des contrôles) pour assurer la conception, le développement, l'installation et l'exploitation sécurisés des systèmes d'information (section 3.2.3). Pour permettre de préciser ce niveau d'effort, le Tableau 9 définit les niveaux 1 à 3 d'assurance de la sécurité en attribuant des exigences à chaque niveau. Les niveaux sont pré-assemblés et proposent des exigences appropriées d'assurance, du niveau rudimentaire au niveau élevé, pour la mise en œuvre des contrôles de sécurité des projets de TI. Les exigences d'assurance de la sécurité sont définies à la prochaine section.

Notons que les profils de contrôle de sécurité de domaine doivent proposer un niveau d'assurance pour la mise en œuvre des contrôles de sécurité afin d'aider les responsables des projets de TI à préciser les exigences d'assurance de la sécurité appropriées.

Tableau 9 : Définitions des niveaux 1 à 3 d'assurance de la sécurité

Identifiant	Type d'exigence d'assurance de la sécurité	Niveaux d'assurance de la sécurité			
		Type de tâche	NAS1	NAS2	NAS3
BNS	Besoins opérationnels en matière de sécurité	Technique	BNS-E-1	BNS-E-1	BNS-E-1 BNS-E-2
		Contenu de la documentation	BNS-D-1 BNS-D-2	BNS-D-1 BNS-D-2	BNS-D-1 BNS-D-2
		Évaluation	BNS-A-1	BNS-A-1	BNS-A-1
SCS	Spécification des contrôles de sécurité	Technique	SCS-E-1	SCS-E-1	SCS-E-1 SCS-E-2
		Contenu de la documentation	SCS-D-1 SCS-D-2	SCS-D-1 SCS-D-2	SCS-D-1 SCS-D-2 SCS-D-3 SCS-D-4
		Évaluation	SCS-A-1	SCS-A-1	SCS-A-1
DS	Spécifications de conception	Technique	DS-E-1	DS-E-1	DS-E-1
		Contenu de la documentation	DS-D-1 DS-D-2	DS-D-1 DS-D-2	DS-D-1 DS-D-2
		Évaluation	DS-A-1 DS-A-2	DS-A-1 DS-A-2	DS-A-1 DS-A-2
TRA	Évaluation des menaces et des risques	Technique	TRA-E-1	TRA-E-1	TRA-E-1 TRA-E-2
		Contenu de la documentation	TRA-D-1 TRA-D-2	TRA-D-1 TRA-D-2 TRA-D-3	TRA-D-1 TRA-D-2 TRA-D-3
		Évaluation	TRA-A-1	TRA-A-1	TRA-A-1

Identifiant	Type d'exigence d'assurance de la sécurité	Niveaux d'assurance de la sécurité			
		Type de tâche	NAS1	NAS2	NAS3
CM	Gestion du changement durant le développement	Technique		CM-E-1 CM-E-2 CM-E-3 CM-E-4	CM-E-1 CM-E-2 CM-E-3 CM-E-5
		Contenu de la documentation		CM-D-1 CM-D-2	CM-D-1 CM-D-2 CM-D-3 CM-D-4 CM-D-5
		Évaluation		CM-A-1 CM-A-2	CM-A-1 CM-A-2 CM-A-3
SM	Mesures de sécurité liées à l'environnement de développement	Technique		SM-E-1	SM-E-1 SM-E-2
		Contenu de la documentation			SM-D-1
		Évaluation		SM-A-1	SM-A-1 SM-A-2
DT	Outils de développement	Technique	DT-E-1	DT-E-1	DT-E-1 DT-E-2
		Contenu de la documentation			DT-D-1 DT-D-2 DT-D-3
		Évaluation	DT-A-1	DT-A-1	DT-A-1 DT-A-2
SDP	Pratiques de développement sécurisées	Technique	SDP-E-1	SDP -E-1 SDP -E-2	SDP -E-1 SDP -E-2
		Contenu de la documentation		SDP-D-1	SDP-D-1
		Évaluation	SDP-A-1	SDP-A-1 SDP-A-2	SDP-A-1 SDP-A-2
ST	Tests de sécurité	Technique	ST-E-1 ST-E-2	ST-E-1 ST-E-2	ST-E-1 ST-E-2 ST-E-3
		Contenu de la documentation	ST-D-1 ST-D-2 ST-D-3	ST-D-1 ST-D-2 ST-D-3	ST-D-1 ST-D-2 ST-D-3 ST-D-4
		Évaluation	ST-A-1	ST-A-1	ST-A-1
OSP	Procédures de sécurité	Technique	OSP-E-1	OSP-E-1	OSP-E-1

Identifiant	Type d'exigence d'assurance de la sécurité	Niveaux d'assurance de la sécurité			
		Type de tâche	NAS1	NAS2	NAS3
	opérationnelles	Contenu de la documentation	OSP-D-1	OSP-D-1 OSP-D-2	OSP-D-1 OSP-D-2 OSP-D-3
		Évaluation	OSP-A-1	OSP-A-1	OSP-A-1
SIP	Procédures d'installation des composants de sécurité	Technique	SIP-E-1	SIP-E-1	SIP-E-1
		Contenu de la documentation	SIP-D-1	SIP-D-1	SIP-D-1
		Évaluation	SIP-A-1	SIP-A-1	SIP-A-1
VA	Évaluation des vulnérabilités	Technique	VA-E-1 VA-E-4	VA-E-1 VA-E-2 VA-E-4 VA-E-5	VA-E-1 VA-E-2 VA-E-3 VA-E-4 VA-E-5
		Contenu de la documentation		VA-D-1	VA-D-1
		Évaluation		VA-A-1	VA-A-1 VA-A-2
SIV	Vérification de l'installation des composants de sécurité	Technique	SIV-E-1 SIV-E-3	SIV-E-2 SIV-E-3 SIV-E-4	SIV-E-2 SIV-E-3 SIV-E-4
		Contenu de la documentation		SIV-D-1	SIV-D-1
		Évaluation	SIV-A-1	SIV-A-1 SIV-A-2	SIV-A-1 SIV-A-2

8.4 Définitions des exigences relatives à l'assurance de la sécurité

8.4.1 BNS – Besoins opérationnels en matière de sécurité

Objectif :

Les besoins opérationnels en matière de sécurité représentent un énoncé administratif concis des besoins de sécurité des processus opérationnels et de l'information connexe que le système d'information prend en charge.

Tâches techniques :

BNS-E-1 Le praticien de la sécurité doit produire un énoncé des besoins opérationnels en matière de sécurité;

BNS-E-2 Le praticien de la sécurité doit produire une justification des besoins opérationnels en matière de sécurité.

Exigences relatives au contenu des documents :

BNS-D-1 L'énoncé des besoins opérationnels en matière de sécurité doit décrire tous les besoins de sécurité associés aux processus opérationnels et à l'information connexe;

BNS-D-2 L'énoncé des besoins opérationnels en matière de sécurité doit tracer chaque besoin opérationnel par rapport aux objectifs organisationnels sous-jacents (p. ex., politique, lois ou obligations contractuelles).

Tâches d'évaluation :

BNS-A-1 L'évaluateur de la sécurité doit confirmer que l'information produite répond à toutes les exigences relatives au contenu des documents.

8.4.2 SCS – Spécification des contrôles de sécurité

Objectif :

La spécification des contrôles de sécurité représente une description claire, non ambiguë et bien définie des contrôles de sécurité applicables.

Tâches techniques :

SCS-E-1 Le praticien de la sécurité doit produire une spécification de contrôle de sécurité;

SCS-E-2 Le praticien de la sécurité doit produire une justification du contrôle de sécurité.

Exigences relatives au contenu des documents :

SCS-D-1 La spécification doit décrire les contrôles de sécurité à un niveau de détail suffisant pour permettre leur attribution durant les phases de conception, et d'une manière non ambiguë pour faciliter le travail du responsable de la conception détaillée;

SCS-D-2 La spécification doit tracer les contrôles de sécurité par rapport aux besoins opérationnels auxquels ils répondent (p. ex., MTES);

SCS-D-3 Tous les termes (sujets, objets, opérations, attributs de sécurité, entités externes et autres) utilisés dans la spécification de contrôle de sécurité doivent être définis;

SCS-D-4 Chaque besoin opérationnel lié à la sécurité doit être respecté. Tout écart doit être expliqué dans une justification du contrôle de sécurité.

Tâches d'évaluation :

SCS-A-1 L'évaluateur de la sécurité doit confirmer que l'information produite répond à toutes les exigences relatives au contenu des documents.

8.4.3 DS – Spécifications de conception

Objectif :

Les spécifications de conception tiennent compte de tous les contrôles de sécurité. Elles servent à guider la mise en œuvre du système d'information.

Tâches techniques :

DS-E-1 Le praticien de la sécurité doit intégrer la conception de la sécurité aux spécifications de conception du système d'information.

Exigences relatives au contenu des documents :

DS-D-1 Les spécifications doivent décrire[14] les éléments de la conception de système qui répondent aux contrôles de sécurité. Exemple : l'application Web utilise le système d'authentification centralisé (c.-à-d. l'élément de conception) pour authentifier l'accès de l'utilisateur (c.-à-d. le contrôle de sécurité);

DS-D-2 Les spécifications doivent tracer[15] la correspondance des éléments de conception par rapport aux contrôles de sécurité auxquels ils répondent.

Tâches d'évaluation :

DS-A-1 L'évaluateur de la sécurité doit confirmer que l'information produite répond à toutes les exigences relatives au contenu des documents;

DS-A-2 L'évaluateur de la sécurité doit s'assurer que les spécifications représentent une instanciation précise et complète de tous les contrôles de sécurité.

[14] Conformément à l'Annexe 5 du guide ITSG-33 (Glossaire) [Référence 11], le terme *décrire* signifie fournir des détails spécifiques sur une entité.

[15] Conformément à l'Annexe 5 du guide ITSG-33 (Glossaire), le terme *tracer* signifie effectuer une analyse informelle de correspondances entre deux entités en appliquant un niveau de rigueur minimal. Cette activité permet de s'assurer que les spécifications de conception traitent toutes les exigences de conception. Une matrice de traçabilité des exigences (MTE) est un bon exemple de ce processus.

8.4.4 TRA – Évaluation des menaces et des risques

Objectif :

La conception de la sécurité du système d'information est soutenue par un processus d'EMR adéquat.

Tâches techniques :

TRA-E-1 Le praticien de la sécurité doit utiliser un processus d'EMR formel établi;

TRA-E-2 Le praticien de la sécurité doit produire une justification de la protection contre les menaces.

Exigences relatives au contenu des documents :

TRA-D-1 La documentation de projet doit décrire les menaces contre lesquelles les biens de TI doivent être protégés;

TRA-D-2 Tous les scénarios de risque doivent être décrits en fonction des biens de TI, des menaces, des vulnérabilités et des niveaux de risque;

TRA-D-3 La documentation de projet doit tracer chaque contrôle ou mécanisme de sécurité par rapport aux menaces qu'il permet de contrer.

Tâches d'évaluation :

TRA-A-1 L'évaluateur de la sécurité doit confirmer que l'information produite répond à toutes les exigences relatives au contenu des documents.

8.4.5 CM – Gestion du changement durant le développement

Objectif :

Tous les changements apportés aux composants du système d'information en développement (p. ex., code source, élément de documentation) sont gérés de manière appropriée.

Tâches techniques :

CM-E-1 L'équipe de développement doit utiliser un système de gestion du changement;

CM-E-2 L'équipe de développement doit produire une documentation sur la gestion du changement;

CM-E-3 L'équipe de développement doit désigner de façon unique tous les éléments de configuration;

CM-E-4 L'équipe de développement doit appliquer des mesures qui font en sorte que seuls des changements autorisés sont apportés aux éléments de configuration;

CM-E-5 L'équipe de développement doit appliquer des mesures automatisées qui font en sorte que seuls des changements autorisés sont apportés aux éléments de configuration.

Exigences relatives au contenu des documents :

CM-D-1 La documentation sur la gestion du changement doit décrire la méthode utilisée pour désigner de façon unique les éléments de configuration.

CM-D-2 La documentation sur la gestion du changement doit décrire les mesures utilisées pour appliquer uniquement les changements autorisés;

CM-D-3 La documentation sur la gestion du changement doit inclure un plan de gestion du changement;

CM-D-4 Le plan de gestion du changement doit décrire la façon d'utiliser le système de gestion du changement pour le développement du système d'information;

CM-D-5 Le plan de gestion du changement doit décrire les procédures utilisées pour accepter des éléments de configuration modifiés ou nouvellement créés.

Tâches d'évaluation :

CM-A-1 L'évaluateur de la sécurité doit confirmer que l'information produite répond à toutes les exigences relatives au contenu des documents;

CM-A-2 L'évaluateur de la sécurité doit confirmer que tous les éléments de configuration sont tenus à jour au moyen du système de gestion du changement;

CM-A-3 L'évaluateur de la sécurité doit confirmer que le système du GC est exploité en conformité avec le plan de gestion du changement.

8.4.6 SM – Mesures de sécurité liées à l'environnement de développement

Objectif :

L'environnement de développement est protégé de manière adéquate sur le plan de la confidentialité, de l'intégrité et de la disponibilité.

Tâches techniques :

SM-E-1 L'équipe de développement doit appliquer des mesures de sécurité pour protéger la confidentialité, l'intégrité et la disponibilité de l'environnement de développement (p. ex., sécurité matérielle, contrôle d'accès, autorisation d'apporter des changements à l'environnement de développement);

SM-E-2 L'équipe de développement doit produire la documentation de sécurité pour l'environnement de développement.

Exigences relatives au contenu des documents :

SM-D-1 La documentation de sécurité doit décrire toutes les mesures de sécurité utilisées pour protéger la confidentialité, l'intégrité et la disponibilité de l'environnement de développement.

Tâches d'évaluation :

SM-A-1 L'évaluateur de la sécurité doit confirmer que les mesures de sécurité sont appliquées;

SM-A-2 L'évaluateur de la sécurité doit confirmer que l'information produite répond à toutes les exigences relatives au contenu des documents.

8.4.7 DT – Outils de développement

Objectif :

L'équipe de développement choisit et utilise les outils de développement appropriés. Ces outils incluent, sans s'y limiter, les langages de programmation, les normes de mise en œuvre et les bibliothèques d'exécution de soutien.

Tâches techniques :

DT-E-1 L'équipe de développement doit sélectionner, installer et configurer les outils appropriés pour le développement du système d'information;

DT-E-2 L'équipe de développement doit produire la documentation pour les outils de développement utilisés.

Exigences relatives au contenu des documents :

DT-D-1 La documentation doit décrire tous outils de développement et indiquer leurs interdépendances et leurs adaptations;

DT-D-2 La documentation de chaque outil de développement doit définir de manière non ambiguë la signification de tous les énoncés ainsi que toutes les conventions et les directives utilisées pour la mise en œuvre;

DT-D-3 La documentation de chaque outil de développement doit définir de manière non ambiguë la signification de toutes les options de mise en œuvre.

Tâches d'évaluation :

DT-A-1 L'évaluateur de la sécurité doit confirmer que les outils de développement appropriés ont été mis en place;

DT-A-2 L'évaluateur de la sécurité doit confirmer que l'information fournie répond à toutes les exigences relatives au contenu des documents.

8.4.8 SDP – Pratiques de développement sécurisées

Objectif :

L'équipe de développement suit les meilleures pratiques en matière de développement sécurisé (p. ex., utilisation des outils et des techniques d'analyse du code source, examen du code source) qui conviennent à son environnement de développement.

Tâches techniques :

SDP-E-1 L'équipe de développement doit suivre les meilleures pratiques en matière de développement sécurisé qui conviennent à son environnement de développement;

SDP-E-2 L'équipe de développement doit produire la documentation qui indique les pratiques de sécurité qu'elle utilise pour développer le système d'information.

Exigences relatives au contenu des documents :

SDP-D-1 La documentation de chaque pratique en matière de développement sécurisé doit inclure des références et décrire le but de la pratique et son utilisation prévue.

Tâches d'évaluation :

SDP-A-1 L'évaluateur de la sécurité doit confirmer que les meilleures pratiques en matière de développement sécurisé sont utilisées;

SDP-A-2 L'évaluateur de la sécurité doit confirmer que l'information produite répond à toutes les exigences relatives au contenu des documents.

8.4.9 ST – Tests de sécurité

Objectif :

S'assurer que les solutions de sécurité du système d'information fonctionnent comme prévu. Les tests de sécurité incluent les tests de développement et d'intégration.

Tâches techniques :

ST-E-1 L'équipe de développement doit tester toutes les solutions de sécurité du système d'information;

ST-E-2 L'équipe de développement doit produire la documentation des tests;

ST-E-3 L'équipe de développement doit produire une analyse des tests de sécurité.

Exigences relatives au contenu des documents :

ST-D-1 La documentation des tests doit inclure des plans de test, les résultats de test prévus et les résultats de test réels;

ST-D-2 Les plans de test doivent indiquer les tests à effectuer et décrire les scénarios d'exécution de chaque test. Les scénarios doivent inclure toutes les interdépendances avec les résultats d'autres tests;

ST-D-3 Les résultats de test réels doivent être conformes aux résultats prévus et tout écart doit être documenté;

ST-D-4 L'analyse des tests de sécurité doit tracer la correspondance entre les tests indiqués dans la documentation des tests et les mécanismes de sécurité précisés dans les spécifications de conception ou les solutions de sécurité indiquées dans la représentation du système d'information.

Tâches d'évaluation :

ST-A-1 L'évaluateur de la sécurité doit confirmer que l'information fournie répond à toutes les exigences relatives au contenu des documents.

8.4.10 OSP – Procédures de sécurité opérationnelles

Objectif :

S'assurer que l'utilisation, l'administration et la maintenance du système d'information sont sécurisées durant la période d'exploitation du système.

Tâches techniques :

OSP-E-1 Le praticien de la sécurité doit produire des procédures de sécurité opérationnelles.

Exigences relatives au contenu des documents :

OSP-D-1 Les procédures de sécurité doivent décrire, pour chaque rôle d'utilisateur, la liste des activités de sécurité à mener pour préserver la sécurité du système d'information dans l'environnement opérationnel (p. ex., le responsable du contrôle d'accès : créer un compte système d'utilisateur final, déverrouiller les comptes, supprimer les comptes inactifs; l'utilisateur final : changer le mot de passe; l'administrateur de systèmes : changer les règles qui gouvernent les mots de passe);

OSP-D-2 Les procédures de sécurité doivent décrire, pour chaque rôle d'utilisateur, la façon d'utiliser les interfaces disponibles (p. ex., l'administrateur de système utilise, à des fins de maintenance, le protocole SSH pour accéder à distance aux serveurs; et l'utilisateur final se connecte à distance);

OSP-D-3 Les procédures de sécurité doivent décrire clairement, pour chaque rôle d'utilisateur, chaque intervention de l'utilisateur et la façon prévue d'intervenir.

Tâches d'évaluation :

OSP-A-1 L'évaluateur de la sécurité doit confirmer que l'information fournie répond à toutes les exigences relatives au contenu des documents.

8.4.11 SIP – Procédures d'installation des composants de sécurité

Objectif :

S'assurer que le système d'information peut être installé de façon sécurisée, en conformité avec la représentation de la mise en œuvre[16].

Tâches techniques :

SIP-E-1 Le praticien de la sécurité doit créer des procédures d'installation des composants de sécurité pour le système d'information.

[16] Conformément à l'Annexe 5 du guide ITSG-33 (Glossaire) [Référence 11], le terme *représentation de la mise en œuvre* signifie la représentation la moins abstraite d'un système d'information. Elle inclut le code source, le matériel et les produits logiciels, les diagrammes de réseau physique, la documentation de configuration tels les manuels de construction, etc. Collectivement, ces éléments permettent de construire le système d'information sans qu'il soit nécessaire de prendre toute autre décision relativement à la conception ou à la mise en œuvre.

Exigences relatives au contenu des documents :

SIP-D-1 Les procédures d'installation des composants de sécurité doivent décrire toutes les étapes nécessaires à la sécurisation de l'installation du système d'information et de la préparation de l'environnement opérationnel.

Tâches d'évaluation :

SIP-A-1 L'évaluateur de la sécurité doit confirmer que l'information fournie répond à toutes les exigences relatives au contenu des documents.

8.4.12 VA – Évaluation des vulnérabilités

Objectif :

Relever et atténuer les vulnérabilités.

Tâches techniques :

VA-E-1 Le praticien de la sécurité doit effectuer une recherche dans les sources du domaine public pour relever les vulnérabilités potentielles du système d'information;

VA-E-2 Le praticien de la sécurité doit effectuer une analyse de vulnérabilités du système d'information au moyen d'un logiciel libre ou disponible dans le commerce pour relever les vulnérabilités potentielles;

VA-E-3 Le praticien de la sécurité doit déterminer, par des tests de pénétration, si les vulnérabilités potentielles relevées peuvent être exploitées par un attaquant;

VA-E-4 Le praticien de la sécurité doit appliquer des rustines et autres mesures correctives pour corriger les vulnérabilités;

VA-E-5 Le praticien de la sécurité doit produire une documentation d'analyse des vulnérabilités.

Exigences relatives au contenu des documents :

VA-D-1 La documentation d'analyse des vulnérabilités doit inclure la liste des vulnérabilités relevées, les rustines et les mesures correctives requises, l'état de l'application des rustines et des mesures correctives dans l'environnement opérationnel et les documents pertinents de la gestion du changement.

Tâches d'évaluation :

VA-A-1 L'évaluateur de la sécurité doit confirmer que l'information fournie répond à toutes les exigences relatives au contenu des documents;

VA-A-2 L'évaluateur de la sécurité doit confirmer, à l'issue d'une inspection de l'environnement opérationnel, l'état de l'application des rustines et des mesures correctives requises.

8.4.13 SIV – Vérification de l'installation des composants de sécurité

Objectif :

Confirmer que les composants de sécurité du système d'information ont été installés et configurés correctement dans l'environnement opérationnel.

Tâches techniques :

SIV-E-1 Le praticien de la sécurité doit effectuer une vérification de l'installation et de la configuration des principaux composants de sécurité dans l'environnement opérationnel du système d'information;

SIV-E-2 Le praticien de la sécurité doit effectuer une vérification approfondie de l'installation et de la configuration des composants de sécurité dans l'environnement opérationnel du système d'information;

SIV-E-3 Le praticien de la sécurité doit corriger les erreurs et les omissions liées à l'installation et à la configuration;

SIV-E-4 Le praticien de la sécurité doit produire la documentation de la vérification de l'installation des composants de sécurité.

Exigences relatives au contenu des documents :

SIV-D-1 La documentation de la vérification de l'installation des composants de sécurité doit inclure un plan de vérification, les résultats prévus de la vérification, les résultats réels, les erreurs d'installation et de configuration relevées, et la confirmation que les erreurs d'installation et de configuration ont été corrigées.

Tâches d'évaluation :

SIV-A-1 L'évaluateur de la sécurité doit confirmer que les erreurs et les omissions liées à l'installation et la configuration ont été corrigées (p. ex., par un examen des documents relatifs à la gestion du changement);

SIV-A-2 L'évaluateur de la sécurité doit confirmer que l'information fournie répond à toutes les exigences relatives au contenu des documents[17].

[17] La combinaison des tâches SIV-E-4 et SIV-A-2 précise les exigences d'assurance de la sécurité des tâches SIV-E-3 SIV-A-1 en exigeant une preuve formelle de l'exécution de toutes les procédures de vérification de la sécurité plutôt que de limiter la preuve à la seule identification et correction des erreurs et des omissions liées à l'installation et à la configuration.

9 Directives sur l'adaptation des contrôles de sécurité

9.1 Introduction

Cette section inclut des directives sur l'adaptation des contrôles de sécurité[18] que l'on doit appliquer durant les étapes de définition, de conception et de développement des systèmes d'information. Les directives sont présentées dans le contexte des projets de TI. Toutefois, elles s'appliquent également au développement des profils de contrôle de sécurité ministérielle et de domaine.

9.2 Aperçu

Au moment de sélectionner des contrôles pour un système particulier à partir d'un profil applicable, les responsables des projets de TI adaptent les contrôles afin de mieux les harmoniser aux conditions particulières du système. Le processus d'adaptation inclut plusieurs activités :

1) Effectuer la sélection initiale des contrôles en suivant les directives sur la définition de la portée;
2) Spécifier les contrôles de compensation, le cas échéant;
3) Spécifier, par des énoncés d'attribution et de sélection explicites, des paramètres de contrôles définis par l'organisation.

Les responsables des projets de TI inscrivent les décisions en matière d'adaptation, y compris les justificatifs pertinents, dans la documentation du système, en conformité avec les exigences d'assurance de la sécurité pertinentes. Ils évaluent et approuvent également ces décisions dans le cadre du processus d'évaluation et d'approbation des contrôles de sécurité du PASSI.

9.3 Directives sur la définition de la portée

Plusieurs facteurs peuvent potentiellement influer sur la façon dont les contrôles s'appliquent à certains systèmes. Ces facteurs sont décrits dans les sous-sections qui suivent.

9.3.1 Facteurs communs associés aux contrôles de sécurité

Les contrôles de sécurité désignés par le SCT ou les autorités de la sécurité ministérielle comme contrôles communs sont, dans la plupart des cas, gérés par une entité ministérielle autre que le propriétaire du système d'information. Les responsables des projets doivent être au fait de l'existence des contrôles de sécurité communs ou de l'obligation de les utiliser. Ils doivent déterminer si ces contrôles s'appliquent au système qu'ils mettent en place et négocier les modalités de leur utilisation.

9.3.2 Facteurs liés à l'exploitation et à l'environnement

Les contrôles de sécurité liés à la nature de l'environnement opérationnel s'appliquent uniquement lorsque le système est déployé dans un environnement qui exige de tels contrôles. Par exemple, certains contrôles

[18] Les procédures d'adaptation sont basées en partie sur les directives énoncées dans le document Special Publication 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations* du NIST [Référence 12].

de sécurité matérielle peuvent ne pas s'appliquer aux systèmes spatiaux, et les contrôles de température et d'humidité peuvent ne pas s'appliquer aux capteurs situés à l'extérieur des installations qui hébergent les systèmes d'information.

9.3.3 Facteurs liés à l'infrastructure physique

Les contrôles liés aux installations ministérielles (p. ex., les contrôles physiques tels les dispositifs de verrouillage et les agents de sécurité; les contrôles environnementaux qui portent sur la température, l'humidité, l'éclairage, l'alimentation et les alarmes d'incendie) ne s'appliquent qu'aux endroits dans les installations qui contribuent directement à la protection ou au soutien des systèmes d'information ou qui leur sont associés.

9.3.4 Facteurs liés à l'accès public

Lorsque le public est autorisé à accéder aux systèmes d'information ministériels, les contrôles de sécurité doivent être appliqués avec discrétion puisque certains contrôles (p. ex., l'identification et l'authentification, les contrôles de sécurité du personnel) peuvent ne pas convenir à ce type d'accès. Par exemple, un profil de domaine peut exiger l'identification et l'authentification des employés du ministère qui assurent la maintenance et le soutien des systèmes qui offrent les services accessibles au public. Par contre, ces mêmes contrôles peuvent ne pas être requis pour accéder aux systèmes par des interfaces publiques et obtenir l'information mise à la disposition des citoyens. D'autre part, les contrôles d'identification et d'authentification peuvent être nécessaires dans certains cas pour les utilisateurs qui accèdent aux systèmes par des interfaces publiques, par exemple, pour accéder à leurs renseignements personnels ou les modifier.

9.3.5 Facteurs liés à la technologie

Les contrôles de sécurité liés à des technologies spécifiques (p. ex., communications sans fil, cryptographie, infrastructure à clé publique) s'appliquent uniquement lorsqu'on les déploie ou qu'on prévoit les déployer dans le système d'information.

Les contrôles s'appliquent uniquement aux composants du système qui appliquent ou soutiennent la capacité de sécurité qui leur est associée et qui présentent les risques potentiels que les contrôles visent à atténuer. Par exemple, les caractéristiques d'un système mono-utilisateur, non lié à un réseau ou qui est relié à un réseau physiquement isolé, peuvent individuellement ou collectivement justifier que l'on n'applique pas certains contrôles de sécurité.

Les contrôles de sécurité doivent, dans la plus grande mesure possible, être appliqués par des mécanismes automatisés. Plusieurs contrôles peuvent être appliqués par des mécanismes déjà prévus dans certains produits commerciaux ou gouvernementaux standards. Par exemple, l'application du contrôle d'accès à certains objets, tels des fichiers, peut être confiée à des mécanismes de contrôle d'accès intégrés aux systèmes d'exploitation. S'il n'existe pas de mécanismes automatisés facilement accessibles pour appliquer un contrôle ou une amélioration, et qu'il n'est pas rentable ou techniquement faisable d'en développer, on doit plutôt utiliser des contrôles de compensation appliqués par des procédures ou des mécanismes non automatisés (voir les modalités d'application des contrôles de compensation ci-dessous).

9.3.6 Facteurs liés aux politiques et aux règlements

Les contrôles de sécurité associés à des exigences obligatoires stipulées dans les lois du GC et les politiques, les directives et les normes du SCT applicables (p. ex., les évaluations des facteurs relatifs à la vie privée) sont requis seulement si leur utilisation est conforme aux types d'information et de système d'information prévus dans ces lois et ces règlements.

9.4 Contrôles de sécurité de compensation

Compte tenu de la nature diversifiée des systèmes d'information actuels, les responsables des projets de TI peuvent juger nécessaire de définir et d'utiliser des contrôles de sécurité de compensation. Ces contrôles sont des contrôles de sécurité opérationnels, techniques ou de gestion que l'on applique au lieu des contrôles de sécurité habituels (d'un profil de contrôle de sécurité applicable) et qui offrent une protection équivalente ou comparable.

Lorsqu'ils envisagent d'utiliser ce type de contrôle pour un système d'information, les responsables doivent respecter les lignes directrices suivantes :

1) Sélectionner, dans la mesure du possible, un contrôle de compensation prévu dans le guide ITSG-33, Annexe 3, *Catalogue des contrôles de sécurité* [Référence 7];
2) Fournir une explication qui justifie la capacité du contrôle à remplir une fonction de sécurité équivalente pour le système d'information et l'impossibilité d'utiliser le contrôle prévu dans le profil de contrôle de sécurité applicable;
3) Évaluer et documenter le risque associé à l'utilisation du contrôle de compensation dans le système d'information.

9.5 Paramètres de contrôle de sécurité définis par l'organisation

Plusieurs des contrôles et des améliorations contiennent des paramètres de contrôle de sécurité définis par l'organisation. Ce sont essentiellement des paramètres substituables que les praticiens de la sécurité, durant le processus de sélection, peuvent remplacer par des valeurs propres au contexte de leur organisation. Ils permettent aux ministères de définir certaines parties d'un contrôle donné pour répondre à des exigences ou des objectifs qui leur sont propres. Ces paramètres peuvent être définis, en tout ou en partie, dans le profil de contrôle de sécurité ministériel ou un profil de contrôle de sécurité de domaine applicable.

Lorsqu'aucun paramètre n'a été défini, les responsables doivent examiner la liste des contrôles de sécurité et, après avoir appliquer les directives sur la définition de la portée et la sélection des contrôles de compensation, déterminer les valeurs appropriées en tenant compte soit des politiques, des directives et des normes de sécurité du ministère et du GC, soit des indications des activités d'EMR ou des meilleures pratiques en matière de sécurité.

10 Références

[Référence 1] Centre de la sécurité des télécommunications. *La gestion des risques liés à la sécurité des TI : Une méthode axée sur le cycle de vie – Activités de gestion des risques liés à la sécurité des TI*. ITSG-33, Annexe 1. 1er novembre 2012.

[Référence 2] Centre de la sécurité des télécommunications. *La gestion des risques liés à la sécurité des TI : Une méthode axée sur le cycle de vie – Aperçu*. ITSG-33. 1er novembre 2012.

[Référence 3] Secrétariat du Conseil du Trésor du Canada. *Politique sur la sécurité du gouvernement*. 1er juillet 2009.

[Référence 4] Secrétariat du Conseil du Trésor du Canada. *Directive sur la gestion de la sécurité ministérielle*. 1er juillet 2009.

[Référence 5] Secrétariat du Conseil du Trésor du Canada. *Norme opérationnelle de sécurité : Gestion de la sécurité des technologies de l'information (GSTI)*. 31 mai 2004.

[Référence 6] Organisation internationale de normalisation (ISO)/Commission électrotechnique internationale (CEI). *Information technology – Systems Security Engineering – Capability Maturity Model (SSE-CMM)*. Numéro de référence ISO/IEC 21827:2002(E), 1er octobre 2002.

[Référence 7] Centre de la sécurité des télécommunications. *La gestion des risques liés à la sécurité des TI : Une méthode axée sur le cycle de vie – Catalogue des contrôles de sécurité*. ITSG-33, Annexe 3. 1er novembre 2012.

[Référence 8] Centre de la sécurité des télécommunications. *Guide sur l'authentification des utilisateurs pour les systèmes TI*. ITSG-31. Mars 2009.

[Référence 9] Organisation internationale de normalisation (ISO)/Commission électrotechnique internationale (CEI). *Information Technology – Security Techniques – Information Security Management Systems – Requirements*. Numéro de référence ISO/IEC 27001:2005. 2005.

[Référence 10] National Security Agency. *Information Assurance Technical Framework*. Release 3.1. Septembre 2002. (*Archivé*)

[Référence 11] Centre de la sécurité des télécommunications. *La gestion des risques liés à la sécurité des TI : Une méthode axée sur le cycle de vie – Glossaire*. ITSG-33, Annexe 5. 1er novembre 2012.

[Référence 12] National Institute of Standards and Technology. *Recommended Security Controls for Federal Information Systems and Organizations*. NIST Special Publication 800-53, révision 3. Août 2009.

[Référence 13] National Institute of Standards and Technology. *Managing Information Security Risk: Organization, Mission, and Information System View*. NIST Special Publication 800-39, mars 2011.