Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada

Conseils en matière de sécurité des technologies de l'information

Détermination des éléments de contrôle en fonction des contrôles de sécurité

ITSG-41 – Annexe 4

Mars 2013

Canada

Avant-propos

Le document *Annexe 4 – Détermination des éléments de contrôle en fonction des contrôles de sécurité* de l'ITSG-41 est un document NON CLASSIFIÉ publié avec l'autorisation du chef du Centre de la sécurité des télécommunications Canada (**CSTC**).

Les propositions de modifications devraient être envoyées au représentant des Services à la clientèle du CSTC 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 du CSTC.

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

Date d'entrée en vigueur

La présente publication entre en vigueur le 2013-03-14.

Signé initialement par

Toni Moffa

Chef adjointe, Sécurité des TI

Historique des révisions

Document n^{o}	Titre	Date de publication
ITSG-41, Annexe 4	Détermination des éléments de contrôle en fonction des contrôles de sécurité	2013-03-14

Table des matières

Liste des figures

Liste des tableaux

Liste des abréviations et acronymes

CSTC	Centre de la sécurité des télécommunications Canada
CDS	Cycle de développement des systèmes
ITSG	Conseils en matière de sécurité des technologies de l'information
PA	Protégé A
PASSI	Processus d'application de la sécurité dans les systèmes d'information
PB	Protégé B
TI	Technologie de l'information
WLAN	Réseau local sans fil

1. Introduction

1.1 But

Le présent document décrit le processus qui permet de sélectionner les éléments de contrôle techniques et axés sur les procédures parmi les contrôles de sécurité sélectionnés durant la phase d'analyse des besoins, décrite dans le document *La gestion des risques liés à la sécurité des TI : Une méthode axée sur le cycle de vie – Aperçu* (**ITSG-33**) [1][1], dans le but :

1) De déterminer les besoins opérationnels en matière de sécurité associés au déploiement des services de *réseau local sans fil* (**WLAN**);

2) De se conformer aux contrôles de sécurité ministériels obligatoires applicables au déploiement des services de réseau local (LAN) sans fil.

Le document inclut des exemples de la façon d'exécuter ce processus en s'appuyant sur les profils de contrôle de sécurité Protégé A/Intégrité faible/Disponibilité faible et Protégé B/Intégrité moyenne/Disponibilité moyenne définis dans le guide ITSG-33 (Annexe 4 - Profil 2 (Protégé A/Intégrité faible/Disponibilité faible) et Annexe 4 - Profil 1 (Protégé B/Intégrité moyenne/Disponibilité moyenne)).

1.2 Auditoire cible

Le document s'adresse aux praticiens des systèmes d'information et de la sécurité et aux responsables des activités de gestion des risques liés à la sécurité des *technologies de l'information* (**IT**) qui interviennent dans la conception et la mise en œuvre des WLAN.

1.3 Structure de la publication

Le document fait partie d'une série de documents qui constituent collectivement la suite de publications ITSG-41. Les autres documents de la série sont les suivants :

- *ITSG-41, Exigences de sécurité liées aux réseaux locaux sans fil* [2]
- *ITSG-41, Annexe 1 – Conception de haut niveau des points d'accès sans fil du gouvernement* [3]
- *ITSG-41, Annexe 2 – Conception de haut niveau – Connexion utilisateur sans fil/réseau câblé* [4]
- *ITSG-41, Annexe 3 – Conception de haut niveau – Interconnexions de réseaux câblés par un pont sans fil* [5]

1 Les numéros entre crochets ([9]) renvoient aux documents de référence qui figurent à la section ***Références*** de la dernière page du document.

2. Éléments de contrôle

Les éléments de contrôle sont déterminés parmi les contrôles de sécurité sélectionnés dans l'Annexe 3, Catalogue des contrôles de sécurité, du guide ITSG-33. L'Annexe 2, Activités de gestion des risques liés à la sécurité des systèmes d'information, décrit également les activités liées à la sécurité qui doivent être exécutées durant le *Cycle de développement des systèmes* (**CDS**) des projets de TI (illustré dans la *Figure 1 - ITSG-33 Cycle de développement des systèmes*) aux fins de conception et de mise en œuvre des mécanismes de contrôle de la sécurité dans les systèmes d'information.

Les activités liées à la sécurité exécutées durant la phase d'analyse des besoins visent la sélection d'un ensemble approuvé de contrôles de sécurité qui permet :

1) De déterminer les besoins opérationnels en matière de sécurité associés au déploiement des services de WLAN;
2) De se conformer aux contrôles de sécurité ministériels obligatoires applicables au déploiement des services de WLAN.

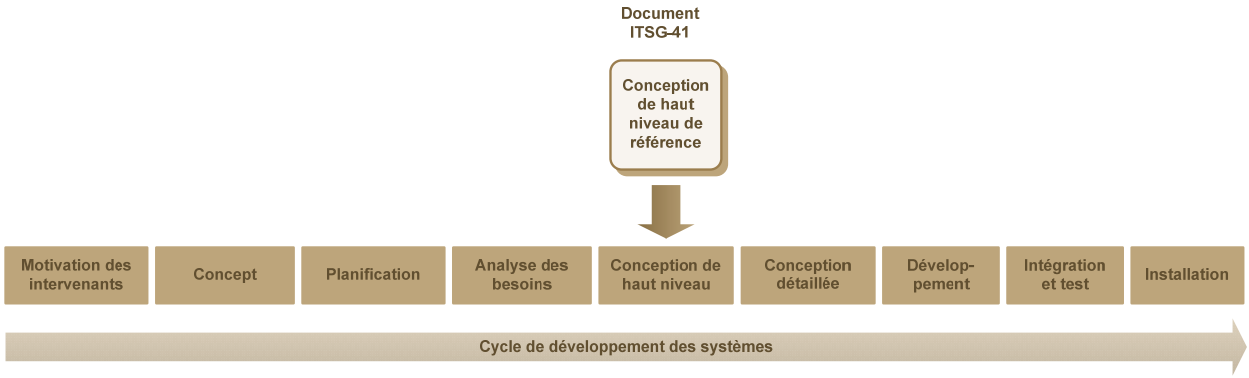

Figure 1 – ITSG-33, Cycle de développement des systèmes

L'ensemble approuvé de contrôles de sécurité pour le déploiement des services de WLAN inclut les classes de contrôles de sécurité techniques, opérationnels et de gestion illustrées dans la *Figure 2 - Contrôles de sécurité et éléments de contrôle* (**Figure 2**) :

1) *Classe des contrôles de sécurité de gestion* - inclut les contrôles qui ne sont pas appliqués dans les systèmes d'information; ils portent principalement sur les activités qui se rapportent à la gestion de la sécurité des TI;
2) *Classe des contrôles de sécurité techniques* - inclut les contrôles normalement appliqués dans les systèmes d'information et exécutés principalement par l'intermédiaire de mécanismes de sécurité qu'on retrouve dans les composants matériels, logiciels et micrologiciels;
3) *Classe des contrôles de sécurité opérationnels* - inclut les contrôles de système d'information qui sont mis en œuvre principalement par l'intermédiaire de processus

exécutés par des personnes (c.-à-d. évaluation de la conformité aux politiques ou exécution de procédures).

Les éléments de contrôle techniques sont d'abord déterminés par l'identification de tous les contrôles de sécurité techniques, opérationnels et de gestion, qui sont ensuite regroupés en contrôles associés à l''environnement d'exploitation et aux systèmes d'information. Par la suite, les contrôles liés aux systèmes d'information sont subdivisés en éléments de contrôle techniques et axés sur les procédures, tel qu'illustré dans la Figure 2 :

1) Les contrôles de sécurité liés aux systèmes d'information peuvent être de nature technique ou axés sur les procédures; leur mise en œuvre relève des propriétaires des systèmes d'information. Ils sont appliqués aux systèmes en recourant à des composants matériels ou logiciels et incluent toutes les procédures manuelles associées à la fonction de sécurité des composants concernés (vérification, journalisation, etc.);

2) Les contrôles de sécurité liés à l'environnement d'exploitation sont essentiellement de nature gestionnelle ou opérationnelle et sont appliqués par des programmes, des politiques ou des procédures ministérielles. Dans certains cas, ils peuvent être mis en œuvre par des moyens techniques ou dans l'infrastructure physique (sécurité matérielle), mais jamais dans les systèmes d'information.

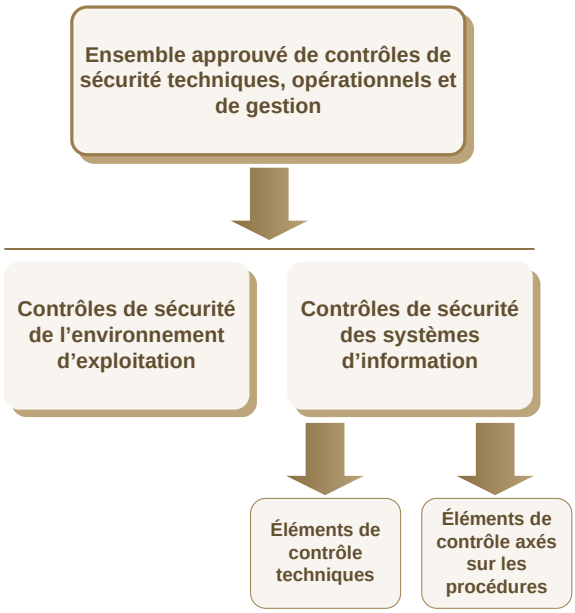

Figure 2 – Contrôles de sécurité et éléments de contrôle

Chaque définition de contrôle de sécurité inclut :

1) Une section « contrôle », qui inclut un ou plusieurs énoncés concis de la capacité de sécurité spécifique nécessaire à la protection d'un aspect particulier du système d'information. Les responsables doivent tenir compte de chaque énoncé, associé à une désignation alphabétique distincte (p. ex. (A), (B), etc.), pour appliquer le contrôle de sécurité;

2) Une section « améliorations » qui inclut, dans un ou plusieurs énoncés concis, les capacités de sécurité supplémentaires qui permettent d'accroître la force du contrôle. Chaque amélioration est associée à une désignation numérique distincte (p. ex. (1), (2), etc.).

Chacun des énoncés de « contrôle » ou d'« améliorations » définit un « élément de contrôle » distinct. Les contrôles de sécurité des systèmes d'information doivent être répartis en éléments de contrôle techniques et axés sur les procédures afin de déterminer la façon dont chaque élément sera appliqué au système d'information.

Les éléments de contrôle techniques proviennent des contrôles de sécurité des systèmes d'information et doivent être appliqués par l'intermédiaire de mécanismes techniques (p. ex. un coupe-feu). Les éléments de contrôle axés sur les procédures proviennent des contrôles de sécurité des systèmes d'information et doivent être appliqués par l'intermédiaire de politiques ou de procédures manuelles (p. ex. l'examen par un employé des journaux de coupe-feu).

2.1 Sélection des éléments de contrôle techniques

Cette section décrit les étapes détaillées, illustrées dans la *Figure 3 – Identification des éléments de contrôle*, nécessaires à la sélection d'éléments de contrôle techniques parmi un ensemble approuvé de contrôles de sécurité déterminés durant la phase d'analyse des besoins du *Processus d'application de la sécurité dans les systèmes d'information* (**PASSI**).

Étape 1 : Une fois que l'ensemble approuvé de contrôles de sécurité a été défini, le *Tableau 1 – Contrôles de sécurité de l'environnement d'exploitation et des systèmes d'information* (**Tableau 1**) permet de départager les contrôles associés à l'environnement d'exploitation de ceux associés aux systèmes d'information;

Étape 2 : Le *Tableau 2 – Éléments de contrôle techniques* (**Tableau 2**) et le *Tableau 3 – Éléments de contrôle axés sur les procédures* (**Tableau 3**) servent à départager les éléments de contrôle techniques des éléments de contrôle axés sur les procédures parmi les contrôles de sécurité des systèmes d'information identifiés à l'*Étape 1*.

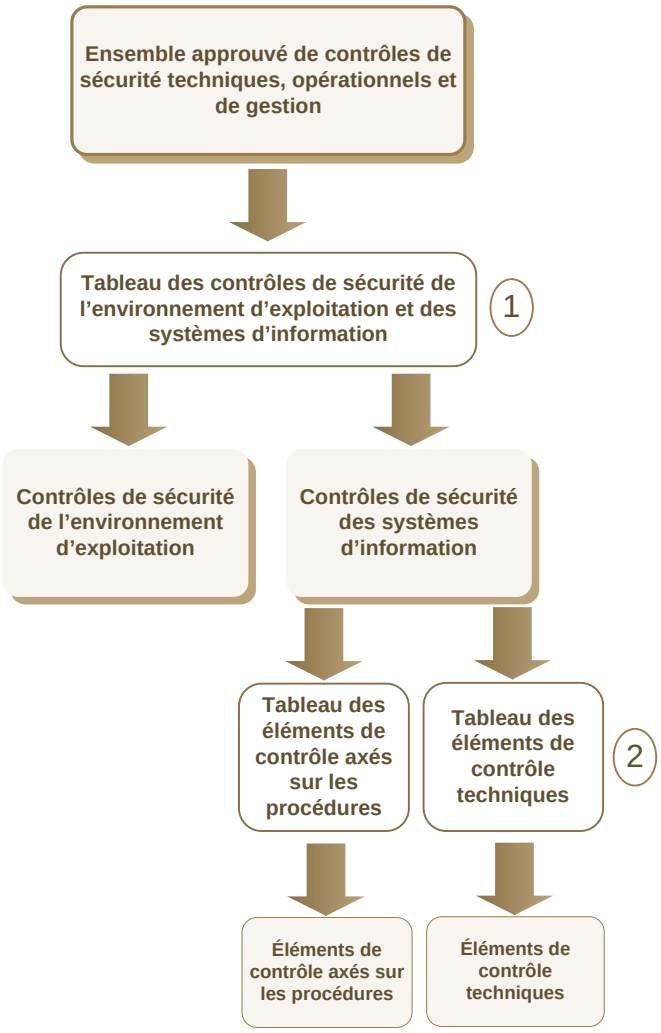

Figure 3 – Identification des éléments de contrôle

Tableau 1 – Contrôles de sécurité de l'environnement d'exploitation et des systèmes d'information

Type de contrôle de sécurité	Numéro de contrôle de sécurité
Environnement d'exploitation	AT-1, AT-2, AT-3, AT-4, AT-5, AU-13, CA-1, CA-2, CA-3, CA-5, CA-6, CA-7, CM-2, CM-3, CM-4, CM-9, CP-2, CP-3, CP-4, CP-6, CP-7, CP-8, IR-1, IR-2, IR-3, IR-4, IR-5, IR-6, IR-7, IR-8, MA-2, MA-3, MA-5, MA-6, MP-2, MP-3, MP-5, PE-1, PE-2, PE-3, PE-4, PE-5, PE-6, PE-7, PE-8, PE-9, PE-10, PE-11, PE-12, PE-13, PE-14, PE-15, PE-16, PE-17, PE-18, PE-19, PL-1, PL-2, PL-4, PL-5, PL-6, PS-1, PS-2, PS-3, PS-4, PS-5, PS-6, PS-7, PS-8, RA-1, RA-2, RA-3, RA-5, SA-1, SA-2, SA-3, SA-4, SA-5, SA-6, SA-7, SA-8, SA-9, SA-10, SA-11, SA-12, SA-13, SA-14, SI-5, SI-12
Système d'information	AC-1, AC-2, AC-3, AC-4, AC-5, AC-6, AC-7, AC-8, AC-9. AC-10, AC-11, AC-14, AC-16, AC-17, AC-18, AC-19, AC-20, AC-21, AC-22, AU-1, AU-2, AU-3, AU-4, AU-5, AU-6, AU-7, AU-8, AU-9, AU-10, AU-11, AU-12, AU-14, CM-1, CM-5, CM-6, CM-7, CM-8, CP-1, CP-9, CP-10, IA-1, IA-2, IA-3, IA-4, IA-5, IA-6, IA-7, IA-8, MA-1, MA-4, MP-1, MP-4, MP-6, SC-1, SC-2, SC-3, SC-4, SC-5, SC-6, SC-7, SC-8, SC-9, SC-10, SC-11, SC-12, SC-13, SC-14, SC-15, SC-16, SC-17, SC-18, SC-19, SC-20, SC-21, SC-22, SC-23, SC-24, SC-25, SC-26, SC-27, SC-28, SC-29, SC-30, SC-31, SC-32, SC-33, SC-34, SC-100, SC-101, SI-1, SI-2, SI-3, SI-4, SI-6, SI-7, SI-8, SI-9, SI-10, SI-11, SI-13

Tableau 2 – Éléments de contrôle techniques

AC-2 Gestion des comptes	AC-2-1, AC-2-2, AC-2-3, AC-2-4, AC-2-5, AC-2-6, AC-2-7
AC-3 Application de l'accès	AC-3-A, AC-3-2, AC-3-3, AC-3-4, AC-3-5, AC-3-6
AC-4 Application des contrôles du flux d'information	AC-4-A, AC-4-1, AC-4-2, AC-4-3, AC-4-4, AC-4-5, AC-4-6, AC-4-7, AC-4-8, AC-4-9, AC-4-10, AC-4-11, AC-4-12, AC-4-13, AC-4-14, AC-4-15, AC-4-17
AC-5 Séparation des tâches	AC-5-C
AC-6 Droit d'accès minimal	AC-6-4
AC-7 Tentatives d'ouverture de session infructueuses	AC-7-A, AC-7-B, AC-7-1, AC-7-2
AC-8 Notification d'utilisation système	AC-8-A, AC-8-B, AC-8-C
AC-9 Notification d'ouverture de session précédente (accès)	AC-9-A, AC-9-1, AC-9-2, AC-9-3
AC-10 Contrôle des sessions simultanées	AC-10-A
AC-11 Verrouillage de session	AC-11-A, AC-11-B, AC-11-1
AC-16 Attributs de sécurité	AC-16-A, AC-16-1, AC-16-2, AC-16-3, AC-16-4, AC-16-5
AC-17 Accès à distance	AC-17-C, AC-17-D, AC-17-E, AC-17-1, AC-17-2, AC-17-3, AC-17-5, C-17-7, AC-17-8, AC-17-100
AC-18 Accès sans fil	AC-18-B, AC-18-C, AC-18-D, AC-18-1, AC-18-2, AC-18-4, AC-18-5
AC-19 Contrôle d'accès pour les dispositifs mobiles	AC-19-B, AC-19-C, AC-19-D, AC-19-E
AC-21 Collaboration et échange d'information entre utilisateurs	AC-21-B, AC-21-1
AU-3 Contenu des enregistrements de vérification	AU-3-A, AU-3-1, AU-3-2
AU-4 Capacité de stockage des vérifications	AU-4-A
AU-5 Intervention en cas d'échecs de vérification	AU-5-A, AU-5-B, AU-5-1, AU-5-2, AU-5-3, AU-5-4
AU-6 Examen, analyse et rapports de vérification	AU-6-3, AU-6-4, AU-6-5
AU-7 Réduction des vérifications et génération de rapports	AU-7-A, AU-7-1
AU-8 Estampilles temporelles	AU-8-A, AU-8-1
AU-9 Protection de l'information	AU-9-A, AU-9-1, AU-9-2, AU-9-3, AU-9-4

de vérification	
AU-10 Non-répudiation	AU-10-A, AU-10-1, AU-10-2, AU-10-3, AU-10-4, AU-10-5
AU-12 Génération d'enregistrements de vérification	AU-12-A, AU-12-B, AU-12-C, AU-12-1, AU-12-2
AU-14 Vérification des sessions	AU-14-A, AU-14-B, AU-14-1
CM-5 Restrictions d'accès associées aux changements	CM-5-A, CM-5-1, CM-5-3, CM-5-6, CM-5-7
CM-6 Paramètres de configuration	CM-6-B, CM-6-1, CM-6-2, CM-6-3
CM-7 Fonctionnalité minimale	CM-7-A, CM-7-2
CM-8 Inventaire des composants de système d'information	CM-8-2, CM-8-3
CP-9 Sauvegarde du système d'information	CP-9-A, CP-9-B, CP-9-C, CP-9-6
CP-10 Reprise et reconstitution du système d'information	CP-10-2, CP-10-5
IA-2 Identification et authentification (utilisateurs organisationnels)	IA-2-A, IA-2-1, IA-2-2, IA-2-3, IA-2-4, IA-2-5, IA-2-6, IA-2-7, IA-2-8, IA-2-9, IA-2-100
IA-3 Identification et authentification des dispositifs	IA-3-A, IA-3-1, IA-3-2
IA-4 Gestion des identificateurs	IA-4-5
IA-5 Gestion des authentifiants	IA-5-1, IA-5-2
IA-6 Rétroaction d'authentification	IA-6-A
IA-7 Authentification des modules cryptographiques	IA-7-A
IA-8 Identification et authentification (utilisateurs non organisationnels)	IA-8-A
MA-4 Télémaintenance	MA-4-C, MA-4-4, MA-4-6, MA-4-7
SC-2 Partitionnement des applications	SC-2-A, SC-2-1
SC-3 Isolement des fonctions de sécurité	SC-3-A, SC-3-1, SC-3-2, SC-3-3, SC-3-4, SC-3-5
SC-4 Information contenue dans les ressources partagées	SC-4-A, SC-4-1

SC-5 Protection contre les dénis de service	SC-5-A, SC-5-1, SC-5-2
SC-6 Priorité des ressources	SC-6-A
SC-7 Protection des frontières	SC-7-A, SC-7-B, SC-7-1, SC-7-2, SC-7-3, SC-7-4, SC-7-5, SC-7-6, SC-7-7, SC-7-8, SC-7-9, SC-7-10, SC-7-11, SC-7-12, SC-7-13, SC-7-15, SC-7-16, SC-7-17, SC-7-18
SC-8 Intégrité des transmissions	SC-8-A, SC-8-1, SC-8-2
SC-9 Confidentialité des transmissions	SC-9-A, SC-9-1, SC-9-2, SC-9-100
SC-10 Déconnexion réseau	SC-10-A
SC-11 Chemin de confiance	SC-11-A
SC-12 Établissement et gestion des clés cryptographiques	SC-12-A, SC-12-2, SC-12-3, SC-12-4, SC12-5
SC-13 Utilisation de la cryptographie	SC-13-A, SC-13-1, SC-13-2, SC-13-3, SC-13-4, SC-13-100, SC-13-101, SC-13-102, SC-13-103, SC-13-104
SC-14 Protection de l'accès public	SC-14-A
SC-15 Dispositifs d'informatique coopérative	SC-15-A, SC-15-B, SC-15-1, SC-15-2
SC-16 Transmission des attributs de sécurité	SC-16-A, SC-16-1
SC-18 Code mobile	SC-18-C, SC-18-1, SC-18-3, SC-18-4
SC-20 Service sécurisé de résolution de nom ou d'adresse (source autorisée)	SC-20-A, SC-20-1
SC-21 Service sécurisé de résolution de nom ou d'adresse (résolveur récursif ou cache)	SC-21-A, SC-21-1
SC-22 Architecture et fourniture de service de résolution de nom ou d'adresse	SC-22-A
SC-23 Authenticité des sessions	SC-23-A, SC-23-1, SC-23-2, SC-23-3, SC-23-4
SC-24 Défaillance dans un état connu	SC-24-A
SC-25 Noeuds légers	SC-25-A
SC-26 Pièges à pirates	SC-26-A, SC-26-1
SC-27 Applications	SC-27-A

indépendantes des systèmes d'exploitation	
SC-28 Protection de l'information inactive	SC-28-A, SC-28-1
SC-29 Hétérogénéité	SC-29-A
SC-30 Techniques de virtualisation	SC-30-A, SC-30-1, SC-30-2
SC-32 Partitionnement des systèmes d'information	SC-32-A
SC-33 Intégrité de la préparation des transmissions	SC-33-A
SC-34 Programmes exécutables non modifiables	SC-34-A, SC-34-B, SC-34-1
SC-100 Authentification de la source	SC-100-A, SC-100-1, SC-100-2, SC-100-3
SC-101 Systèmes de télécommunications non classifiés dans les installations sécurisées	SC-101-A, SC-101-B, SC-101-C, SC-101-D
SI-2 Correction des défauts	SI-2-1, SI-2-2, SI-2-4
SI-3 Protection contre les codes malveillants	SI-3-A, SI-3-C, SI-3-1, SI-3-2, SI-3-3, SI-3-4
SI-4 Surveillance des systèmes d'information	SI-4-A, SI-4-C, SI-4-1, SI-4-2, SI-4-3, SI-4-4, SI-4-5, SI-4-6, SI-4-7, SI-4-8, SI-4-10, SI-4-11, SI-4-12, SI-4-13, SI-4-14, SI-4-15
SI-6 Vérification de la fonctionnalité de sécurité	SI-6-A, SI-6-1 SI-6-2
SI-7 Intégrité de l'information et des logiciels	SI-7-A, SI-7-2, SI-7-3
SI-8 Protection antipourriel	SI-8-A, SI-8-1, SI-8-2
SI-9 Restrictions relatives à la saisie d'information	SI-9-A
SI-10 Validation de la saisie d'information	SI-10-A
SI-11 Traitement des erreurs	SI-11-A, SI-11-B, SI-11-C

Tableau 3 – Éléments de contrôle axés sur les procédures

Type de contrôle de sécurité	Numéro du contrôle de sécurité
AC-2 Gestion des comptes	AC-2-1, AC-2-2, AC-2-3, AC-2-4, AC-2-5, AC-2-6, AC-2-7
AC-3 Application de l'accès	AC-3-A, AC-3-2, AC-3-3, AC-3-4, AC-3-5, AC-3-6
AC-4 Application des contrôles du flux d'information	AC-4-A, AC-4-1, AC-4-2, AC-4-3, AC-4-4, AC-4-5, AC-4-6, AC-4-7, AC-4-8, AC-4-9, AC-4-10, AC-4-11, AC-4-12, AC-4-13, AC-4-14, AC-4-15, AC-4-17
AC-5 Séparation des tâches	AC-5-C
AC-6 Droit d'accès minimal	AC-6-4
AC-7 Tentatives d'ouverture de session infructueuses	AC-7-A, AC-7-B, AC-7-1, AC-7-2
AC-8 Notification d'utilisation système	AC-8-A, AC-8-B, AC-8-C
AC-9 Notification d'ouverture de session précédente (accès)	AC-9-A, AC-9-1, AC-9-2, AC-9-3
AC-10 Contrôle des sessions simultanées	AC-10-A
AC-11 Verrouillage de session	AC-11-A, AC-11-B, AC-11-1
AC-16 Attributs de sécurité	AC-16-A, AC-16-1, AC-16-2, AC-16-3, AC-16-4, AC-16-5
AC-17 Accès à distance	AC-17-C, AC-17-D, AC-17-E, AC-17-1, AC-17-2, AC-17-3, AC-17-5, C-17-7, AC-17-8, AC-17-100
AC-18 Accès sans fil	AC-18-B, AC-18-C, AC-18-D, AC-18-1, AC-18-2, AC-18-4, AC-18-5
AC-19 Contrôle d'accès pour les dispositifs mobiles	AC-19-B, AC-19-C, AC-19-D, AC-19-E
AC-21 Collaboration et échange d'information entre utilisateurs	AC-21-B, AC-21-1
AU-3 Contenu des enregistrements de vérification	AU-3-A, AU-3-1, AU-3-2
AU-4 Capacité de stockage des vérifications	AU-4-A
AU-5 Intervention en cas d'échecs de vérification	AU-5-A, AU-5-B, AU-5-1, AU-5-2, AU-5-3, AU-5-4
AU-6 Examen, analyse et rapports de vérification	AU-6-3, AU-6-4, AU-6-5
AU-7 Réduction des vérifications et génération de rapports	AU-7-A, AU-7-1
AU-8 Estampilles temporelles	AU-8-A, AU-8-1

Type de contrôle de sécurité	Numéro du contrôle de sécurité
AU-9 Protection de l'information de vérification	AU-9-A, AU-9-1, AU-9-2, AU-9-3, AU-9-4
AU-10 Non-répudiation	AU-10-A, AU-10-1, AU-10-2, AU-10-3, AU-10-4, AU-10-5
AU-12 Génération d'enregistrements de vérification	AU-12-A, AU-12-B, AU-12-C, AU-12-1, AU-12-2
AU-14 Vérification des sessions	AU-14-A, AU-14-B, AU-14-1
CM-5 Restrictions d'accès associées aux changements	CM-5-A, CM-5-1, CM-5-3, CM-5-6, CM-5-7
CM-6 Paramètres de configuration	CM-6-B, CM-6-1, CM-6-2, CM-6-3
CM-7 Fonctionnalité minimale	CM-7-A, CM-7-2
CM-8 Inventaire des composants de système d'information	CM-8-2, CM-8-3
CP-9 Sauvegarde du système d'information	CP-9-A, CP-9-B, CP-9-C, CP-9-6
CP-10 Reprise et reconstitution du système d'information	CP-10-2, CP-10-5
IA-2 Identification et authentification (utilisateurs organisationnels)	IA-2-A, IA-2-1, IA-2-2, IA-2-3, IA-2-4, IA-2-5, IA-2-6, IA-2-7, IA-2-8, IA-2-9, IA-2-100
IA-3 Identification et authentification des dispositifs	IA-3-A, IA-3-1, IA-3-2
IA-4 Gestion des identificateurs	IA-4-5
IA-5 Gestion des authentifiants	IA-5-1, IA-5-2
IA-6 Rétroaction d'authentification	IA-6-A
IA-7 Authentification des modules cryptographiques	IA-7-A
IA-8 Identification et authentification (utilisateurs non organisationnels)	IA-8-A
MA-4 Télémaintenance	MA-4-C, MA-4-4, MA-4-6, MA-4-7
SC-2 Partitionnement des applications	SC-2-A, SC-2-1
SC-3 Isolement des fonctions de sécurité	SC-3-A, SC-3-1, SC-3-2, SC-3-3, SC-3-4, SC-3-5

Type de contrôle de sécurité	Numéro du contrôle de sécurité
SC-4 Information contenue dans les ressources partagées	SC-4-A, SC-4-1
SC-5 Protection contre les dénis de service	SC-5-A, SC-5-1, SC-5-2
SC-6 Priorité des ressources	SC-6-A
SC-7 Protection des frontières	SC-7-A, SC-7-B, SC-7-1, SC-7-2, SC-7-3, SC-7-4, SC-7-5, SC-7-6, SC-7-7, SC-7-8, SC-7-9, SC-7-10, SC-7-11, SC-7-12, SC-7-13, SC-7-15, SC-7-16, SC-7-17, SC-7-18
SC-8 Intégrité des transmissions	SC-8-A, SC-8-1, SC-8-2
SC-9 Confidentialité des transmissions	SC-9-A, SC-9-1, SC-9-2, SC-9-100
SC-10 Déconnexion réseau	SC-10-A
SC-11 Chemin de confiance	SC-11-A
SC-12 Établissement et gestion des clés cryptographiques	SC-12-A, SC-12-2, SC-12-3, SC-12-4, SC12-5
SC-13 Utilisation de la cryptographie	SC-13-A, SC-13-1, SC-13-2, SC-13-3, SC-13-4, SC-13-100, SC-13-101, SC-13-102, SC-13-103, SC-13-104
SC-14 Protection de l'accès public	SC-14-A
SC-15 Dispositifs d'informatique coopérative	SC-15-A, SC-15-B, SC-15-1, SC-15-2
SC-16 Transmission des attributs de sécurité	SC-16-A, SC-16-1
SC-18 Code mobile	SC-18-C, SC-18-1, SC-18-3, SC-18-4
SC-20 Service sécurisé de résolution de nom ou d'adresse (source autorisée)	SC-20-A, SC-20-1
SC-21 Service sécurisé de résolution de nom ou d'adresse (résolveur récursif ou cache)	SC-21-A, SC-21-1
SC-22 Architecture et fourniture de service de résolution de nom ou d'adresse	SC-22-A
SC-23 Authenticité des sessions	SC-23-A, SC-23-1, SC-23-2, SC-23-3, SC-23-4
SC-24 Défaillance dans un état connu	SC-24-A
SC-25 Noeuds légers	SC-25-A

Type de contrôle de sécurité	Numéro du contrôle de sécurité
SC-26 Pièges à pirates	SC-26-A, SC-26-1
SC-27 Applications indépendantes des systèmes d'exploitation	SC-27-A
SC-28 Protection de l'information inactive	SC-28-A, SC-28-1
SC-29 Hétérogénéité	SC-29-A
SC-30 Techniques de virtualisation	SC-30-A, SC-30-1, SC-30-2
SC-32 Partitionnement des systèmes d'information	SC-32-A
SC-33 Intégrité de la préparation des transmissions	SC-33-A
SC-34 Programmes exécutables non modifiables	SC-34-A, SC-34-B, SC-34-1
SC-100 Authentification de la source	SC-100-A, SC-100-1, SC-100-2, SC-100-3
SC-101 Systèmes de télécommunications non classifiés dans les installations sécurisées	SC-101-A, SC-101-B, SC-101-C, SC-101-D
SI-2 Correction des défauts	SI-2-1, SI-2-2, SI-2-4
SI-3 Protection contre les codes malveillants	SI-3-A, SI-3-C, SI-3-1, SI-3-2, SI-3-3, SI-3-4
SI-4 Surveillance des systèmes d'information	SI-4-A, SI-4-C, SI-4-1, SI-4-2, SI-4-3, SI-4-4, SI-4-5, SI-4-6, SI-4-7, SI-4-8, SI-4-10, SI-4-11, SI-4-12, SI-4-13, SI-4-14, SI-4-15
SI-6 Vérification de la fonctionnalité de sécurité	SI-6-A, SI-6-1 SI-6-2
SI-7 Intégrité de l'information et des logiciels	SI-7-A, SI-7-2, SI-7-3
SI-8 Protection antipourriel	SI-8-A, SI-8-1, SI-8-2
SI-9 Restrictions relatives à la saisie d'information	SI-9-A
SI-10 Validation de la saisie d'information	SI-10-A
SI-11 Traitement des erreurs	SI-11-A, SI-11-B, SI-11-C

2.2 Exemple : profil Protégé A/Intégrité faible/Disponibilité faible

Cette section utilise le profil de contrôle de sécurité Protégé A/Intégrité faible/Disponibilité faible défini dans le guide ITSG-33 (Annexe 4 - Profil 2) comme ensemble approuvé de contrôles de sécurité au cours du processus de sélection des éléments de contrôle techniques défini à la *Section 2.1 Sélection des éléments de contrôle techniques*. Les résultats du processus sont indiqués.

Étape 1 : Le Tableau 1 permet de déterminer les contrôles de sécurité du profil de contrôle de sécurité Protégé A/Intégrité faible/Disponibilité faible qui sont des contrôles liés à l'environnement d'exploitation et ceux qui sont liés aux systèmes d'information. Les résultats figurent dans le *Tableau 4 – Contrôles de sécurité de l'environnement d'exploitation et des systèmes d'information du profil PA/F/F* (**Tableau 4**);

Étape 2 : Le Tableau 2 et le Tableau 3 permettent de déterminer les éléments de contrôle techniques et axés sur les procédures parmi les contrôles de sécurité des systèmes d'information identifiés dans le Tableau 4. Les résultats figurent dans le *Tableau 5 – Éléments de contrôle techniques du profil PA/F/F* et le *Tableau 6 – Éléments de contrôle axés sur les procédures du profil PA/F/F*, respectivement.

Tableau 4 – Contrôles de sécurité de l'environnement d'exploitation et des systèmes d'information du profil PA/F/F

Type de contrôle de sécurité	Numéro du contrôle de sécurité
Environnement d'exploitation	AT-1, AT-2, AT-3, AT-4, CA-1, CA-2, CA-3, CA-5, CA-6, CA-7, CM-2, CM-3, CM-4, CM-9, CP-2, CP-3, IR-1, IR-2, IR-4, IR-6, IR-7, IR-8, MA-2, MA-5, MP-2, MP-3, PE-1, PE-2, PE-3, PE-6, PE-7, PE-8, PE-10, PE-11, PE-12, PE-13, PE-14, PE-15, PE-16, PE-18, PL-1, PL-2, PL-4, PL-5, PL-6, PS-1, PS-2, PS-3, PS-4, PS-5, PS-6, PS-7, PS-8, RA-1, RA-2, RA-3, RA-5, SA-1, SA-2, SA-3, SA-4, SA-5, SA-6, SA-7, SA-8, SA-9, SA-12, SI-5, SI-12
Système d'information	AC-1, AC-2, AC-3, AC-4, AC-5, AC-6, AC-7, AC-8, AC-9. AC-11, AC-14, AC-16, AC-17, AC-18, AC-19, AC-20, AC-21, AC-22, AU-1, AU-2, AU-3, AU-4, AU-6, AU-8, AU-9, AU-11, AU-12, CM-1, CM-5, CM-6, CM-7, CM-8, CP-1, CP-9, CP-10, IA-1, IA-2, IA-3, IA-4, IA-5, IA-6, IA-7, IA-8, MA-1, MA-4, MP-1, MP-6, SC-1, SC-2, SC-7, SC-10, SC-12, SC-13, SC-14, SC-15, SC-17, SC-18, SC-19, SC-22, SC-23, SC-24, SC-28, SI-1, SI-2, SI-3, SI-4, SI-8, SI-10

Tableau 5 – Éléments de contrôle techniques du profil PA/F/F

Type de contrôle de sécurité	Numéro du contrôle de sécurité
AC-2 Gestion des comptes	AC-2-1, AC-2-2, AC-2-3, AC-2-4, AC-2-5
AC-3 Application de l'accès	AC-3-A, AC-3-4
AC-4 Application des contrôles du flux d'information	AC-4-A
AC-5 Séparation des tâches	AC-5-C
AC-6 Droit d'accès minimal	S.O.
AC-7 Tentatives d'ouverture de session infructueuses	AC-7-A, AC-7-B
AC-8 Notification d'utilisation système	AC-8-A, AC-8-B, AC-8-C
AC-9 Notification d'ouverture de session précédente (accès)	AC-9-A, AC-9-1, AC-9-2, AC-9-3
AC-10 Contrôle des sessions simultanées	S.O.
AC-11 Verrouillage de session	AC-11-A, AC-11-B, AC-11-1
AC-16 Attributs de sécurité	AC-16-A, AC-16-2, AC-16-4, AC-16-5
AC-17 Accès à distance	AC-17-C, AC-17-D, AC-17-E, AC-17-1, AC-17-2, AC-17-3, AC-17-5, C-17-7, AC-17-8, AC-17-100
AC-18 Accès sans fil	AC-18-B, AC-18-C, AC-18-D, AC-18-1, AC-18-2, AC-18-4
AC-19 Contrôle d'accès pour les dispositifs mobiles	AC-19-B, AC-19-C, AC-19-D, AC-19-E
AC-21 Collaboration et échange d'information entre utilisateurs	AC-21-B
AU-3 Contenu des enregistrements de vérification	AU-3-A, AU-3-1
AU-4 Capacité de stockage des vérifications	AU-4-A
AU-5 Intervention en cas d'échecs de vérification	AU-5-A, AU-5-B, AU-5-1
AU-6 Examen, analyse et rapports de vérification	S.O.
AU-7 Réduction des vérifications et génération de rapports	S.O.
AU-8 Estampilles temporelles	AU-8-A, AU-8-1

Type de contrôle de sécurité	Numéro du contrôle de sécurité
AU-9 Protection de l'information de vérification	AU-9-A, AU-9-4
AU-10 Non-répudiation	S.O.
AU-12 Génération d'enregistrements de vérification	AU-12-A, AU-12-B, AU-12-C
AU-14 Vérification des sessions	S.O.
CM-5 Restrictions d'accès associées aux changements	CM-5-A, CM-5-1, CM-5-6
CM-6 Paramètres de configuration	CM-6-B, CM-6-3
CM-7 Fonctionnalité minimale	CM-7-A
CM-8 Inventaire des composants de système d'information	CM-8-2, CM-8-3
CP-9 Sauvegarde du système d'information	CP-9-A, CP-9-B, CP-9-C
CP-10 Reprise et reconstitution du système d'information	S.O.
IA-2 Identification et authentification (utilisateurs organisationnels)	IA-2-A, IA-2-8, IA-2-9, IA-2-100
IA-3 Identification et authentification des dispositifs	IA-3-A, IA-3-1
IA-4 Gestion des identificateurs	S.O.
IA-5 Gestion des authentifiants	IA-5-1, IA-5-2
IA-6 Rétroaction d'authentification	IA-6-A
IA-7 Authentification des modules cryptographiques	IA-7-A
IA-8 Identification et authentification (utilisateurs non organisationnels)	IA-8-A
MA-4 Télémaintenance	MA-4-C
SC-2 Partitionnement des applications	SC-2-A, SC-2-1
SC-3 Isolement des fonctions de sécurité	S.O.

Type de contrôle de sécurité	Numéro du contrôle de sécurité
SC-4 Information contenue dans les ressources partagées	S.O.
SC-5 Protection contre les dénis de service	S.O.
SC-6 Priorité des ressources	S.O.
SC-7 Protection des frontières	SC-7-A, SC-7-B, SC-7-1, SC-7-2, SC-7-3, SC-7-4, SC-7-5, SC-7-6, SC-7-7, SC-7-8, SC-7-9, SC-7-11, SC-7-12, SC-7-13, SC-7-18
SC-8 Intégrité des transmissions	S.O.
SC-9 Confidentialité des transmissions	S.O.
SC-10 Déconnexion réseau	SC-10-A
SC-11 Chemin de confiance	S.O.
SC-12 Établissement et gestion des clés cryptographiques	SC-12-A
SC-13 Utilisation de la cryptographie	SC-13-A, SC-13-4
SC-14 Protection de l'accès public	SC-14-A
SC-15 Dispositifs d'informatique coopérative	SC-15-A, SC-15-B, SC-15-2
SC-16 Transmission des attributs de sécurité	S.O.
SC-18 Code mobile	SC-18-C, SC-18-1, SC-18-3, SC-18-4
SC-20 Service sécurisé de résolution de nom ou d'adresse (source autorisée)	S.O.
SC-21 Service sécurisé de résolution de nom ou d'adresse (résolveur récursif ou cache)	S.O.
SC-22 Architecture et fourniture de service de résolution de nom ou d'adresse	SC-22-A
SC-23 Authenticité des sessions	SC-23-A, SC-23-1, SC-23-2, SC-23-3, SC-23-4
SC-24 Défaillance dans un état connu	SC-24-A
SC-25 Noeuds légers	S.O.

Type de contrôle de sécurité	Numéro du contrôle de sécurité
SC-26 Pièges à pirates	S.O.
SC-27 Applications indépendantes des systèmes d'exploitation	S.O.
SC-28 Protection de l'information inactive	SC-28-A
SC-29 Hétérogénéité	S.O.
SC-30 Techniques de virtualisation	S.O.
SC-32 Partitionnement des systèmes d'information	S.O.
SC-33 Intégrité de la préparation des transmissions	S.O.
SC-34 Programmes exécutables non modifiables	S.O.
SC-100 Authentification de la source	S.O.
SC-101 Systèmes de télécommunications non classifiés dans les installations sécurisées	S.O.
SI-2 Correction des défauts	S.O.
SI-3 Protection contre les codes malveillants	SI-3-A, SI-3-C, SI-3-1, SI-3-2, SI-3-3, SI-3-4
SI-4 Surveillance des systèmes d'information	SI-4-A, SI-4-C, SI-4-5, SI-4-6, SI-4-7, SI-4-8, SI-4-10, SI-4-11
SI-6 Vérification de la fonctionnalité de sécurité	S.O.
SI-7 Intégrité de l'information et des logiciels	S.O.
SI-8 Protection antipourriel	SI-8-A, SI-8-1, SI-8-2
SI-9 Restrictions relatives à la saisie d'information	S.O.
SI-10 Validation de la saisie d'information	SI-10-A
SI-11 Traitement des erreurs	S.O.

Tableau 6 – Éléments de contrôle axés sur les procédures du profil PA/F/F

Type de contrôle de sécurité	Numéro du contrôle de sécurité
AC-1 Politique et procédures de contrôle d'accès	AC-1-A, AC-1-B
AC-2 Gestion des comptes	AC-2-A, AC-2-B, AC-2-C, AC-2-D, AC-2-E, AC-2-F, AC-2-G, AC-2-H, AC-2-I , AC-2-J
AC-4 Application des contrôles du flux d'information	S.O.
AC-5 Séparation des tâches	AC-5-A, AC-5-B
AC-6 Droit d'accès minimal	AC-6-A, AC-6-1, AC-6-2, AC-6-5
AC-14 Opérations permises sans identification ni authentification	AC-14-A, AC-14-B, AC-14-1
AC-17 Accès à distance	AC-17-A, AC-17-B, AC-17-AA, AC-17-4, AC-17-6
AC-18 Accès sans fil	AC-18-A, AC-18-3
AC-19 Contrôle d'accès pour les dispositifs mobiles	AC-19-A, AC-19-F, AC-19-G, AC-19-1, AC-19-2, AC-19-3
AC-20 Utilisation de systèmes d'information externes	AC-20-A, AC-20-B
AC-21 Collaboration et échange d'information entre utilisateurs	AC-21-A, AC-21-100
AC-22 Contenu accessible au public	AC-22-A, AC-22-B, AC-22-C, AC-22-D, AC-22-E
AU-1 Politique et procédures de vérification et de responsabilisation	AU-1-A, AU-1-B
AU-2 Événements vérifiables	AU-2-A, AU-2-B, AU-2-C, AU-2-D, AU-2-3, AU-2-4
AU-6 Examen, analyse et rapports de vérification	AU-6-A, AU-6-B, AU-6-1
AU-11 Conservation des enregistrements de vérification	AU-11-A
CM-1 Politique et procédures de gestion des configurations	CM-1-A, CM-1-B
CM-5 Restrictions d'accès associées aux changements	CM-5-2, CM-5-5
CM-6 Paramètres de configuration	CM-6-A, CM-6-C, CM-6-D, CM-6-4,
CM-7 Fonctionnalité minimale	CM-7-1, CM-7-3

Type de contrôle de sécurité	Numéro du contrôle de sécurité
CM-8 Inventaire des composants de système d'information	CM-8-A, CM-8-B, CM-8-C, CM-8-D, CM-8-E, CM-8-1, CM-8-4, CM-8-5
CP-1 Politique et procédures de planification d'urgence	CP-1-A, CP-1-B, CP-1-AA
CP-9 Sauvegarde du système d'information	CP-9-D, CP-9-1
CP-10 Reprise et reconstitution du système d'information	CP-10-A
IA-1 Politique et procédures d'identification et d'authentification	IA-1-A, IA-1-B
IA-3 Identification et authentification des dispositifs	IA-3-3
IA-4 Gestion des identificateurs	IA-4-A, IA-4-B, IA-4-C, IA-4-D, IA-4-E, IA-4-2, IA-4-3, IA-4-4
IA-5 Gestion des authentifiants	IA-5-A, IA-5-B, IA-5-C, IA-5-D, IA-5-E, IA-5-F, IA-5-G, IA-5-H, IA-5-I, IA-5-3, IA-5-6, IA-5-7, IA-5-8
MA-1 Politique et procédures de maintenance des systèmes	MA-1-A, MA-1-B
MA-4 Télémaintenance	MA-4-A, MA-4-B, MA-4-D
MP-4 Entreposage des supports	S.O.
SC-1 Politique et procédures de protection des systèmes et des communications	SC-1-A, SC-1-B
SC-7 Protection des frontières	S.O.
SC-12 Établissement et gestion des clés cryptographiques	SC-12-1
SC-15 Dispositifs d'informatique coopérative	SC-15-3
SC-17 Certificats d'infrastructure à clé publique	SC-17-A
SC-18 Code mobile	SC-18-A, SC-18-B, SC-18-2
SC-19 Voix sur protocole internet	SC-19-A, SC-19-B
SC-31 Analyse des voies clandestines	S.O.
SC-34 Programmes exécutables non modifiables	S.O.

Type de contrôle de sécurité	Numéro du contrôle de sécurité
SI-1 Politique et procédures liées à l'intégrité de l'information et des systèmes	SI-1-A, SI-1-B
SI-2 Correction des défauts	SI-2-A, SI-2-B, SI-2-C
SI-3 Protection contre les codes malveillants	SI-3-B, SI-3-D, SI-3-5, SI-3-6
SI-4 Surveillance des systèmes d'information	SI-4-B, SI-4-D, SI-4-E, SI-4-9
SI-6 Vérification de la fonctionnalité de sécurité	S.O.
SI-7 Intégrité de l'information et des logiciels	S.O.
SI-8 Protection antipourriel	SI-8-B
SI-13 Prévention des pannes prévisibles	S.O.

2.3 Exemple : profil Protégé B/Intégrité moyenne/Disponibilité moyenne

Cette section utilise le profil de contrôle de sécurité Protégé B/Intégrité moyenne/Disponibilité moyenne défini dans le guide ITSG-33 (Annexe 4 - Profil 1) comme ensemble approuvé de contrôles de sécurité au cours du processus de sélection des éléments de contrôle techniques défini à la *Section 2.1 Sélection des éléments de contrôle techniques*. Les résultats du processus sont indiqués.

Étape 1 : Le Tableau 1 permet de déterminer les contrôles de sécurité du profil de contrôle de sécurité Protégé B/Intégrité moyenne/Disponibilité moyenne qui sont des contrôles liés à l'environnement d'exploitation et ceux qui sont liés aux systèmes d'information. Les résultats figurent dans le *Tableau 4 – Contrôles de sécurité de l'environnement d'exploitation et des systèmes d'information du profil PB/M/M* (**Tableau 7**);

Étape 2 : Le Tableau 2 et le Tableau 3 permettent de déterminer les éléments de contrôle techniques et axés sur les procédures parmi les contrôles de sécurité des systèmes d'information identifiés dans le Tableau 7. Les résultats figurent dans le *Tableau 8 – Éléments de contrôle techniques du profil PB/M/M* et le *Tableau 9 – Éléments de contrôle axés sur les procédures du profil PB/M/M*, respectivement.

Tableau 7 – Contrôles de sécurité de l'environnement d'exploitation et des systèmes d'information du profil PB/M/M

Type de contrôle de sécurité	Numéro du contrôle de sécurité
Environnement d'exploitation	AT-1, AT-2, AT-3, AT-4, CA-1, CA-2, CA-3, CA-5, CA-6, CA-7, CM-2, CM-3, CM-4, CM-9, CP-2, CP-3, IR-1, IR-2, IR-4, IR-6, IR-7, IR-8, MA-2, MA-5, MP-2, MP-3, PE-1, PE-2, PE-3, PE-6, PE-7, PE-8, PE-10, PE-11, PE-12, PE-13, PE-14, PE-15, PE-16, PE-18, PL-1, PL-2, PL-4, PL-5, PL-6, PS-1, PS-2, PS-3, PS-4, PS-5, PS-6, PS-7, PS-8, RA-1, RA-2, RA-3, RA-5, SA-1, SA-2, SA-3, SA-4, SA-5, SA-6, SA-7, SA-8, SA-9, SA-12, SI-5, SI-12
Système d'information	AC-1, AC-2, AC-3, AC-4, AC-5, AC-6, AC-7, AC-8, AC-9. AC-11, AC-14, AC-16, AC-17, AC-18, AC-19, AC-20, AC-21, AC-22, AU-1, AU-2, AU-3, AU-4, AU-6, AU-8, AU-9, AU-11, AU-12, CM-1, CM-5, CM-6, CM-7, CM-8, CP-1, CP-9, CP-10, IA-1, IA-2, IA-3, IA-4, IA-5, IA-6, IA-7, IA-8, MA-1, MA-4, MP-1, MP-6, SC-1, SC-2, SC-7, SC-10, SC-12, SC-13, SC-14, SC-15, SC-17, SC-18, SC-19, SC-22, SC-23, SC-24, SC-28, SI-1, SI-2, SI-3, SI-4, SI-8, SI-10

Tableau 8 – Éléments de contrôle techniques du profil PB/M/M

Type de contrôle de sécurité	Numéro du contrôle de sécurité
AC-2 Gestion des comptes	AC-2-1, AC-2-2, AC-2-3, AC-2-4, AC-2-5, AC-2-7
AC-3 Application de l'accès	AC-3-A, AC-3-4
AC-4 Application des contrôles du flux d'information	AC-4-A
AC-5 Séparation des tâches	AC-5-C
AC-6 Droit d'accès minimal	S.O.
AC-7 Tentatives d'ouverture de session infructueuses	AC-7-A, AC-7-B
AC-8 Notification d'utilisation système	AC-8-A, AC-8-B, AC-8-C
AC-9 Notification d'ouverture de session précédente (accès)	AC-9-A, AC-9-1, AC-9-2, AC-9-3
AC-10 Contrôle des sessions simultanées	S.O.
AC-11 Verrouillage de session	AC-11-A, AC-11-B, AC-11-1
AC-16 Attributs de sécurité	AC-16-A, AC-16-2, AC-16-4, AC-16-5
AC-17 Accès à distance	AC-17-C, AC-17-D, AC-17-E, AC-17-1, AC-17-2, AC-17-3, AC-17-5, C-17-7, AC-17-8, AC-17-100
AC-18 Accès sans fil	AC-18-B, AC-18-C, AC-18-D, AC-18-1, AC-18-2, AC-18-4
AC-19 Contrôle d'accès pour les dispositifs mobiles	AC-19-B, AC-19-C, AC-19-D, AC-19-E
AC-21 Collaboration et échange d'information entre utilisateurs	AC-21-B
AU-3 Contenu des enregistrements de vérification	AU-3-A, AU-3-1
AU-4 Capacité de stockage des vérifications	AU-4-A
AU-5 Intervention en cas d'échecs de vérification	AU-5-A, AU-5-B, AU-5-1
AU-6 Examen, analyse et rapports de vérification	AU-6-3, AU-6-4
AU-7 Réduction des vérifications et génération de rapports	AU-7-A, AU-7-1
AU-8 Estampilles temporelles	AU-8-A, AU-8-1

Type de contrôle de sécurité	Numéro du contrôle de sécurité
AU-9 Protection de l'information de vérification	AU-9-A, AU-9-2, AU-9-4
AU-10 Non-répudiation	S.O.
AU-12 Génération d'enregistrements de vérification	AU-12-A, AU-12-B, AU-12-C, AU-12-1, AU-12-2
AU-14 Vérification des sessions	S.O.
CM-5 Restrictions d'accès associées aux changements	CM-5-A, CM-5-1, CM-5-6, CM-5-7
CM-6 Paramètres de configuration	CM-6-B, CM-6-1, CM-6-2, CM-6-3
CM-7 Fonctionnalité minimale	CM-7-A, CM-7-2
CM-8 Inventaire des composants de système d'information	CM-8-2, CM-8-3
CP-9 Sauvegarde du système d'information	CP-9-A, CP-9-B, CP-9-C
CP-10 Reprise et reconstitution du système d'information	CP-10-2
IA-2 Identification et authentification (utilisateurs organisationnels)	IA-2-A, IA-2-8, IA-2-9, IA-2-100
IA-3 Identification et authentification des dispositifs	IA-3-A, IA-3-1
IA-4 Gestion des identificateurs	S.O.
IA-5 Gestion des authentifiants	IA-5-1, IA-5-2
IA-6 Rétroaction d'authentification	IA-6-A
IA-7 Authentification des modules cryptographiques	IA-7-A
IA-8 Identification et authentification (utilisateurs non organisationnels)	IA-8-A
MA-4 Télémaintenance	MA-4-C, MA-4-4, MA-4-6
SC-2 Partitionnement des applications	SC-2-A, SC-2-1
SC-3 Isolement des fonctions de sécurité	S.O.

Type de contrôle de sécurité	Numéro du contrôle de sécurité
SC-4 Information contenue dans les ressources partagées	S.O.
SC-5 Protection contre les dénis de service	SC-5-A, SC-5-2
SC-6 Priorité des ressources	S.O.
SC-7 Protection des frontières	SC-7-A, SC-7-B, SC-7-1, SC-7-2, SC-7-3, SC-7-4, SC-7-5, SC-7-6, SC-7-7, SC-7-8, SC-7-9, SC-7-11, SC-7-12, SC-7-13, SC-7-18
SC-8 Intégrité des transmissions	SC-8-A, SC-8-1
SC-9 Confidentialité des transmissions	SC-9-A, SC-9-1
SC-10 Déconnexion réseau	SC-10-A
SC-11 Chemin de confiance	S.O.
SC-12 Établissement et gestion des clés cryptographiques	SC-12-A
SC-13 Utilisation de la cryptographie	SC-13-A, SC-13-4
SC-14 Protection de l'accès public	SC-14-A
SC-15 Dispositifs d'informatique coopérative	SC-15-A, SC-15-B, SC-15-2
SC-16 Transmission des attributs de sécurité	S.O.
SC-18 Code mobile	SC-18-C, SC-18-1, SC-18-3
SC-20 Service sécurisé de résolution de nom ou d'adresse (source autorisée)	S.O.
SC-21 Service sécurisé de résolution de nom ou d'adresse (résolveur récursif ou cache)	S.O.
SC-22 Architecture et fourniture de service de résolution de nom ou d'adresse	SC-22-A
SC-23 Authenticité des sessions	SC-23-A, SC-23-1, SC-23-2, SC-23-3, SC-23-4
SC-24 Défaillance dans un état connu	SC-24-A
SC-25 Noeuds légers	S.O.

Type de contrôle de sécurité	Numéro du contrôle de sécurité
SC-26 Pièges à pirates	S.O.
SC-27 Applications indépendantes des systèmes d'exploitation	S.O.
SC-28 Protection de l'information inactive	SC-28-A
SC-29 Hétérogénéité	SC-29-A
SC-30 Techniques de virtualisation	S.O.
SC-32 Partitionnement des systèmes d'information	S.O.
SC-33 Intégrité de la préparation des transmissions	S.O.
SC-34 Programmes exécutables non modifiables	S.O.
SC-100 Authentification de la source	S.O.
SC-101 Systèmes de télécommunications non classifiés dans les installations sécurisées	S.O.
SI-2 Correction des défauts	S.O.
SI-3 Protection contre les codes malveillants	SI-3-A, SI-3-C, SI-3-1, SI-3-2, SI-3-3, SI-3-4
SI-4 Surveillance des systèmes d'information	SI-4-A, SI-4-C, SI-4-1, SI-4-2, SI-4-3, SI-4-4, SI-4-5, SI-4-6, SI-4-7, SI-4-8, SI-4-10, SI-4-11, SI-4-12, SI-4-13, SI-4-14, SI-4-15
SI-6 Vérification de la fonctionnalité de sécurité	S.O.
SI-7 Intégrité de l'information et des logiciels	SI-7-A, SI-7-2, SI-7-3
SI-8 Protection antipourriel	SI-8-A, SI-8-1, SI-8-2
SI-9 Restrictions relatives à la saisie d'information	SI-9-A
SI-10 Validation de la saisie d'information	SI-10-A
SI-11 Traitement des erreurs	SI-11-A, SI-11-B, SI-11-C

Tableau 9 – Éléments de contrôle axés sur les procédures du profil PB/M/M

Type de contrôle de sécurité	Numéro du contrôle de sécurité
AC-1 Politique et procédures de contrôle d'accès	AC-1-A, AC-1-B
AC-2 Gestion des comptes	AC-2-A, AC-2-B, AC-2-C, AC-2-D, AC-2-E, AC-2-F, AC-2-G, AC-2-H, AC-2-I , AC-2-J
AC-4 Application des contrôles du flux d'information	S.O.
AC-5 Séparation des tâches	AC-5-A, AC-5-B
AC-6 Droit d'accès minimal	AC-6-A, AC-6-1, AC-6-2, AC-6-5
AC-14 Opérations permises sans identification ni authentification	AC-14-A, AC-14-B, AC-14-1
AC-17 Accès à distance	AC-17-A, AC-17-B, AC-17-AA, AC-17-4, AC-17-6
AC-18 Accès sans fil	AC-18-A, AC-18-3
AC-19 Contrôle d'accès pour les dispositifs mobiles	AC-19-A, AC-19-F, AC-19-G, AC-19-1, AC-19-2, AC-19-3, AC-19-100
AC-20 Utilisation de systèmes d'information externes	AC-20-A, AC-20-B, AC-20-1, AC-20-2
AC-21 Collaboration et échange d'information entre utilisateurs	AC-21-A, AC-21-100
AC -22 Contenu accessible au public	AC-22-A, AC-22-B, AC-22-C, AC-22-D, AC-22-E
AU-1 Politique et procédures de vérification et de responsabilisation	AU-1-A, AU-1-B
AU-2 Événements vérifiables	AU-2-A, AU-2-B, AU-2-C, AU-2-D, AU-2-3, AU-2-4
AU-6 Examen, analyse et rapports de vérification	AU-6-A, AU-6-B, AU-6-1, AU-6-7
AU-11 Conservation des enregistrements de vérification	AU-11-A
CM-1 Politique et procédures de gestion des configurations	CM-1-A, CM-1-B
CM-5 Restrictions d'accès associées aux changements	CM-5-2, CM-5-5
CM-6 Paramètres de configuration	CM-6-A, CM-6-C, CM-6-D, CM-6-4
CM-7 Fonctionnalité minimale	CM-7-1, CM-7-3

Type de contrôle de sécurité	Numéro du contrôle de sécurité
CM-8 Inventaire des composants de système d'information	CM-8-A, CM-8-B, CM-8-C, CM-8-D, CM-8-E, CM-8-1, CM-8-4, CM-8-5, CM-8-6
CP-1 Politique et procédures de planification d'urgence	CP-1-A, CP-1-B, CP-1-AA
CP-9 Sauvegarde du système d'information	CP-9-D, CP-9-1, CP-9-2, CP-9-3, CP-9-5
CP-10 Reprise et reconstitution du système d'information	CP-10-A, CP-10-4, CP-10-6
IA-1 Politique et procédures d'identification et d'authentification	IA-1-A, IA-1-B
IA-3 Identification et authentification des dispositifs	IA-3-3
IA-4 Gestion des identificateurs	IA-4-A, IA-4-B, IA-4-C, IA-4-D, IA-4-E, IA-4-1, IA-4-2, IA-4-3, IA-4-4
IA-5 Gestion des authentifiants	IA-5-A, IA-5-B, IA-5-C, IA-5-D, IA-5-E, IA-5-F, IA-5-G, IA-5-H, IA-5-I, IA-5-3, IA-5-6, IA-5-7, IA-5-8
MA-1 Politique et procédures de maintenance des systèmes	MA-1-A, MA-1-B
MA-4 Télémaintenance	MA-4-A, MA-4-B, MA-4-D, MA-4-1, MA-4-2, MA-4-3, MA-4-5
MP-4 Entreposage des supports	MP-4-A, MP-4-B, MP-4-1
SC-1 Politique et procédures de protection des systèmes et des communications	SC-1-A, SC-1-B
SC-7 Protection des frontières	S.O.
SC-12 Établissement et gestion des clés cryptographiques	SC-12-1
SC-15 Dispositifs d'informatique coopérative	SC-15-3
SC-17 Certificats d'infrastructure à clé publique	SC-17-A
SC-18 Code mobile	SC-18-A, SC-18-B, SC-18-2
SC-19 Voix sur protocole internet	SC-19-A, SC-19-B
SC-31 Analyse des voies clandestines	S.O.
SC-34 Programmes exécutables non modifiables	S.O.

Type de contrôle de sécurité	Numéro du contrôle de sécurité
SI-1 Politique et procédures liées à l'intégrité de l'information et des systèmes	SI-1-A, SI-1-B
SI-2 Correction des défauts	SI-2-A, SI-2-B, SI-2-C
SI-3 Protection contre les codes malveillants	SI-3-B, SI-3-D, SI-3-5, SI-3-6
SI-4 Surveillance des systèmes d'information	SI-4-B, SI-4-D, SI-4-E, SI-4-9
SI-6 Vérification de la fonctionnalité de sécurité	S.O.
SI-7 Intégrité de l'information et des logiciels	SI-7-1, SI-7-4
SI-8 Protection antipourriel	SI-8-B
SI-13 Prévention des pannes prévisibles	S.O.

3. Références

[1] *ITSG-33, La gestion des risques liés à la sécurité des TI : Une méthode axée sur le cycle de vie – Aperçu ;* **CSTC** (nov 2012)

[2] *ITSG-41, Exigences de sécurité liées aux réseaux locaux sans fil*; **CSTC** (mars 2013)

[3] *ITSG-41, Annexe 1 – Conception de haut niveau des points d'accès sans fil du gouvernement*; **CSTC** (mars 2013)

[4] *ITSG-41, Annexe 2 – Conception de haut niveau – Connexion utilisateur sans fil/réseau câblé*; **CSTC** (mars 2013)

[5] *ITSG-41, Annexe 3 – Conception de haut niveau – Interconnexions de réseaux câblés par un pont sans fil*; **CSTC** (mars 2013)