



Centre de la sécurité
des télécommunications

Communications
Security Establishment

CENTRE CANADIEN POUR LA **CYBERSÉCURITÉ**

Évaluation des exigences visant la sécurité de l'information désignée

Praticien·nes

Vue d'ensemble

Le présent document est une version canadienne de la publication du National Institute of Standards and Technology (NIST) intitulée [SP 800-171A Rev. 3 Assessing Security Requirements for Controlled Unclassified Information](#) (en anglais seulement). Il fournit un ensemble complet de procédures visant à évaluer les exigences de sécurité et se veut une ligne directrice complémentaire au document *Protection de l'information désignée dans les organisations et les systèmes ne relevant pas du gouvernement du Canada* (ITSP.10.171).

La protection de l'information désignée revêt une importance capitale pour les ministères et organismes du gouvernement du Canada (GC). Elle peut avoir une incidence directe sur la capacité du GC de mener à bien ses missions et ses fonctions essentielles. Cette publication offre aux ministères et aux organismes du GC des procédures d'évaluation des exigences de sécurité recommandées visant à protéger la confidentialité de l'information désignée lorsqu'elle se trouve dans des organisations et des systèmes ne relevant pas du GC. Ces procédures d'évaluation s'appliquent aux exigences de sécurité établies par les organismes et organismes du GC dans les mécanismes de passation de marchés ou les autres ententes mises en place entre les organisations ne relevant pas du GC et ces ministères et organismes. Les organisations peuvent utiliser les procédures d'évaluation pour produire la preuve que les exigences de sécurité indiquées dans les ententes et les contrats ont bien été respectées.

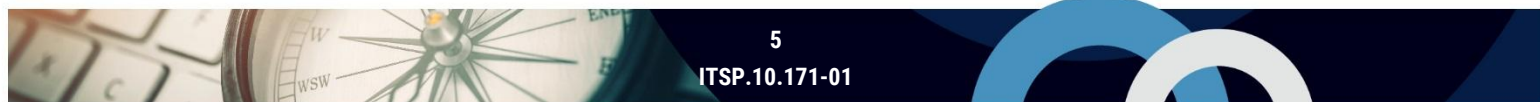
Mentions

Le Centre pour la cybersécurité souhaite remercier Victoria Pillitteri et Ron Ross (PhD) de la division de sécurité informatique du NIST d'avoir permis à l'équipe des Conseils en matière de cybersécurité (CSG pour *Cyber Security Guidance*) d'utiliser leurs conseils et de les modifier afin de les adapter au contexte canadien.

Table des matières

1	Introduction	10
1.1	Objet.....	10
1.2	Public cible	10
1.3	Structure de la publication	11
2	Principes de base	12
2.1	Procédures d'évaluation	12
2.2	Cas d'assurance.....	16
3	Procédures	19
3.1	Contrôle d'accès	19
03.01.01	Gestion des comptes	19
03.01.02	Application de l'accès	21
03.01.03	Application du contrôle de flux d'information	22
03.01.04	Séparation des tâches.....	22
03.01.05	Droit d'accès minimal	23
03.01.06	Droit d'accès minimal – Comptes privilégiés	24
03.01.07	Droit d'accès minimal – Fonctions privilégiées	25
03.01.08	Tentatives d'ouverture de session infructueuses	25
03.01.09	Avis d'utilisation système.....	26
03.01.10	Verrouillage d'appareil	27
03.01.11	Fin de session	28
03.01.12	Accès à distance	28
03.01.13	Non affecté	29
03.01.14	Non affecté	29
03.01.15	Non affecté	29
03.01.16	Accès sans fil	30
03.01.17	Non affecté	30
03.01.18	Contrôle d'accès pour les appareils mobiles	31
03.01.19	Non affecté	31

03.01.20	Utilisation de systèmes externes	31
03.01.21	Non affecté	32
03.01.22	Contenu accessible au public	33
3.2	Sensibilisation et formation	33
03.02.01	Formation et sensibilisation en matière de sécurité.....	33
03.02.02	Formation selon le rôle	35
03.02.03	Non affecté	36
3.3	Vérification et responsabilisation.....	36
03.03.01	Journalisation d'événements.....	36
03.03.02	Contenu des enregistrements de vérification	37
03.03.03	Génération d'enregistrements de vérification	38
03.03.04	Intervention en cas d'échec du processus de journalisation des données de vérification.....	39
03.03.05	Examen, analyse et production de rapports liés aux enregistrements de vérification.....	40
03.03.06	Réduction des enregistrements de vérification et génération de rapports	41
03.03.07	Horodatage	41
03.03.08	Protection de l'information de vérification	42
03.03.09	Non affecté	43
3.4	Gestion des configurations.....	43
03.04.01	Configuration de référence.....	43
03.04.02	Paramètres de configuration	44
03.04.03	Contrôle des changements de configuration	45
03.04.04	Analyses des répercussions	46
03.04.05	Restrictions d'accès associées aux changements	47
03.04.06	Fonctionnalité minimale.....	47
03.04.07	Non affecté	49
03.04.08	Logiciels autorisés – Autorisation par exception	49
03.04.09	Non affecté	50
03.04.10	Inventaire des composants du système	50
03.04.11	Localisation de l'information	51
03.04.12	Configuration des systèmes et des composants pour des zones à risque élevé.....	52



3.5	Identification et authentification	52
03.05.01	Identification, authentification et réauthentification des utilisatrices et utilisateurs	53
03.05.02	Identification et authentification des dispositifs.....	53
03.05.03	Authentification multifacteur.....	54
03.05.04	Authentification résistant à la réinsertion.....	55
03.05.05	Gestion des identifiants	55
03.05.06	Non affecté	56
03.05.07	Gestion des mots de passe	56
03.05.08	Non affecté	57
03.05.09	Non affecté	57
03.05.10	Non affecté	57
03.05.11	Réinjection d'authentification	58
03.05.12	Gestion des authentifiants	58
3.6	Intervention en cas d'incident	59
03.06.01	Traitement des incidents.....	60
03.06.02	Surveillance des incidents, signalement des incidents et assistance en cas d'incident.....	61
03.06.03	Tests d'intervention en cas d'incident	62
03.06.04	Formation sur les interventions en cas d'incident	62
03.06.05	Plan d'intervention en cas d'incident.....	63
3.7	Maintenance	64
03.07.01	Non affecté	64
03.07.02	Non affecté	65
03.07.03	Non affecté	65
03.07.04	Outils de maintenance	65
03.07.05	Maintenance non locale	66
03.07.06	Personnel de maintenance	66
3.8	Protection des supports	67
03.08.01	Entreposage des supports.....	67
03.08.02	Accès aux supports	68
03.08.03	Nettoyage des supports	69

03.08.04	Marquage des supports	69
03.08.05	Transport des supports	70
03.08.06	Non affecté	71
03.08.07	Utilisation des supports	71
03.08.08	Non affecté	72
03.08.09	Sauvegarde du système – Protection cryptographique.....	72
3.9	Sécurité du personnel	72
03.09.01	Filtrage de sécurité du personnel	72
03.09.02	Cessation d'emploi et mutation de personnel	73
3.10	Protection matérielle	74
03.10.01	Autorisations d'accès physique	74
03.10.02	Surveillance de l'accès physique	75
03.10.03	Non affecté	76
03.10.04	Non affecté	76
03.10.05	Non affecté	76
03.10.06	Autres lieux de travail	76
03.10.07	Contrôle d'accès physique	77
03.10.08	Contrôle d'accès pour la transmission	78
3.11	Évaluation des risques	79
03.11.01	Évaluation des risques	79
03.11.02	Surveillance et analyse des vulnérabilités	80
03.11.03	Non affecté	81
03.11.04	Réponse aux risques	81
3.12	Évaluation de sécurité et surveillance	82
03.12.01	Évaluation de sécurité	82
03.12.02	Plans d'action et des jalons	82
03.12.03	Surveillance continue	83
03.12.04	Non affecté	84
03.12.05	Échange d'information	84
3.13	Protection des systèmes et des communications	85

03.13.01	Protection des frontières.....	85
03.13.02	Non affecté	86
03.13.03	Non affecté	86
03.13.04	Information dans les ressources système partagées	86
03.13.05	Non affecté	87
03.13.06	Communications réseau – Refus par défaut et autorisation par exception.....	87
03.13.07	Non affecté	87
03.13.08	Confidentialité lors de la transmission et du stockage.....	87
03.13.09	Déconnexion du réseau	88
03.13.10	Établissement et gestion des clés cryptographiques	89
03.13.11	Protection cryptographique	90
03.13.12	Applications et dispositifs d’informatique collaborative.....	90
03.13.13	Code mobile	91
03.13.14	Non affecté	92
03.13.15	Authenticité des sessions	92
03.13.16	Non affecté	92
3.14	Intégrité de l’information et des systèmes	93
03.14.01	Correction des défauts.....	93
03.14.02	Protection contre les programmes malveillants.....	94
03.14.03	Alertes, avis et directives de sécurité.....	95
03.14.04	Non affecté	96
03.14.05	Non affecté	96
03.14.06	Surveillance des systèmes	96
03.14.07	Non affecté	97
03.14.08	Gestion et conservation de l’information.....	97
3.15	Planification	98
03.15.01	Politique et procédures	98
03.15.02	Plan de sécurité du système.....	99
03.15.03	Règles de conduite	100
3.16	Acquisition des systèmes et des services	101

03.16.01	Principes d'ingénierie de la sécurité des systèmes	101
03.16.02	Composants de systèmes non pris en charge	102
03.16.03	Services de systèmes externes.....	103
3.17	Gestion des risques liés à la chaîne d'approvisionnement.....	104
03.17.01	Plan de gestion des risques liés à la chaîne d'approvisionnement	104
03.17.02	Stratégies, outils et méthodes d'acquisition	105
03.17.03	Exigences et processus de la chaîne d'approvisionnement	106
A.1	Paramètres définis par l'organisation	108

Liste des figures

Figure 1 :	Structure et contenu d'une procédure d'évaluation.....	15
------------	--	----

Liste des tableaux

Tableau 1 :	Paramètres définis par l'organisation	108
-------------	---	-----

Introduction

Le présent document est une version canadienne de la publication [NIST, SP 800-171A Rev. 3 Assessing Security Requirements for Controlled Unclassified Information](#) (en anglais seulement). Il n'y a pas de changements techniques importants entre la publication canadienne et le document SP 800-171A Rev. 3. Les principales modifications concernent les différences entre les lois, les politiques, les directives, les normes et les lignes directrices. Autrement dit, les changements tiennent compte du contexte réglementaire et de conformité propre au Canada; aucun changement n'a été apporté au contexte technique sous-jacent.

Le processus d'évaluation de sécurité vise à rassembler l'information et à fournir des preuves pour déterminer l'efficacité des exigences de sécurité en faisant ce qui suit :

- cerner les problèmes ou les lacunes dans les programmes de gestion des risques et de la sécurité;
- définir les faiblesses et les lacunes en matière de sécurité dans les systèmes et les environnements où s'exécutent ces systèmes;
- établir les priorités liées aux décisions et aux activités d'atténuation des risques;
- confirmer que les faiblesses et les lacunes relevées par rapport à la sécurité dans le système et l'environnement d'exploitation ont bien été corrigées;
- soutenir les activités de surveillance continue et assurer une connaissance de la situation concernant la sécurité de l'information.

1.1 Objet

Cette publication fournit un ensemble complet de procédures visant à évaluer l'efficacité des exigences de sécurité pour protéger la confidentialité de l'information désignée lorsqu'elle réside dans des systèmes et des organisations qui ne relèvent pas du GC. Les lignes directrices s'appliquent aux exigences de sécurité définies dans le document *Protection de l'information désignée dans les organisations et les systèmes ne relevant pas du gouvernement du Canada* (ITSP.10.171).

L'objectif principal de l'évaluation est de s'assurer que les contrôles de sécurité sont mis en œuvre avec une robustesse et une ampleur suffisantes pour contrer les auteurs de menaces identifiés.

1.2 Public cible

Cette publication est destinée aux personnes et aux organisations des secteurs publics et privés, y compris :

- les responsables du cycle de développement des systèmes, par exemple :
 - les gestionnaires de programme;
 - les responsables de la mission ou des activités;
 - les gardiennes et gardiens de l'information;
 - les conceptrices et concepteurs de systèmes;

- les ingénieures et ingénieurs en sécurité des systèmes;
- les intégratrices et intégrateurs de systèmes;
- les responsables des acquisitions et de l'approvisionnement (par exemple, les agentes et agents de négociation des marchés);
- les responsables de la gestion et de la surveillance des systèmes, de la sécurité, de la protection de la vie privée ou des risques, par exemple :
 - les responsables de l'autorisation;
 - les dirigeantes principales et dirigeants principaux de l'information;
 - les dirigeantes principales et dirigeants principaux de la sécurité de l'information;
 - les chefs de la protection des renseignements personnels;
 - les propriétaires de systèmes;
 - les gestionnaires de la sécurité de l'information;
- les responsables de l'évaluation et de la surveillance de la sécurité ou de la protection de la vie privée, par exemple :
 - les vérificatrices et vérificateurs;
 - les évaluatrices et évaluateurs de systèmes;
 - les contrôleuses et contrôleurs;
 - les vérificatrices indépendantes, les vérificateurs indépendants et les responsables de la validation;
 - les analystes.

On peut aborder les rôles et les responsabilités ci-dessus selon deux perspectives :

- celle du GC où l'entité définit et applique les exigences relatives à l'évaluation de sécurité dans des mécanismes de passation de marchés ou d'autres types d'ententes;
- celle adoptée à l'extérieur du GC où les exigences relatives à l'évaluation de sécurité sont établies dans les contrats ou les ententes par l'entité responsable d'y répondre et de s'y conformer.

1.3 Structure de la publication

La suite de cette publication sera structurée comme suit :

- [Section 2 : Principes de base](#) : décrit les concepts fondamentaux associés aux évaluations des exigences de sécurité, ce qui comprend les procédures, les méthodes et les objets d'évaluation, ainsi que les cas d'assurance, qu'il est possible de créer à partir des preuves produites au cours de l'évaluation;
- [Section 3 : Procédures](#) : fournit les procédures d'évaluation relatives aux exigences de sécurité de l'ITSP.10.171, dont les objectifs de l'évaluation et les objectifs et les objets d'évaluation potentiels pour chaque procédure;
- [Annexe A : Paramètres définis par l'organisation](#) : fournit des renseignements supplémentaires pour appuyer la protection de l'information désignée.

2 Principes de base

Le processus utilisé par les organisations et les contrôleuses et contrôleurs pour évaluer les exigences de sécurité mentionnées dans l'ITSP.10.171-01 comprend les étapes suivantes :

1. la préparation de l'évaluation;
2. l'élaboration d'un plan d'évaluation de la sécurité et de la protection de la vie privée;
3. la réalisation de l'évaluation;
4. la documentation, l'analyse et la présentation des résultats de l'évaluation.

Le document *Évaluation des contrôles et des activités d'assurance de la sécurité et de la protection de la vie privée* (ITSP.10.033-02) fournit de l'information additionnelle sur le processus d'évaluation et chacune des étapes mentionnées ci-dessus.

Cette section décrit la structure et le contenu des procédures d'évaluation, ainsi que l'importance de faire appel à des cas d'assurance afin de fournir les preuves nécessaires pour établir la conformité avec les exigences.

2.1 Procédures d'évaluation

Les exigences de sécurité de l'ITSP.10.171 représentent un sous-ensemble des contrôles nécessaires à la protection de la confidentialité de l'information désignée. Les exigences de sécurité sont organisées en 17 familles. Chaque famille contient les exigences associées au sujet de sécurité d'ordre général qu'elle aborde. Les procédures d'évaluation mentionnées à la [section 3](#) sont regroupées en fonction des désignations de leurs familles pour assurer le caractère exhaustif et l'uniformité des évaluations. Les procédures sont tirées des procédures d'évaluation de l'ITSP.10.033-02.

La liste qui suit donne les familles d'exigences de sécurité :

- Contrôle d'accès
- Sensibilisation et formation
- Vérification et responsabilisation
- Gestion des configurations
- Identification et authentification
- Intervention en cas d'incident
- Maintenance
- Protection des supports
- Sécurité du personnel
- Protection matérielle
- Évaluation des risques
- Évaluation de sécurité et surveillance
- Protection des systèmes et des communications

- Intégrité de l'information et des systèmes
- Planification
- Acquisition des systèmes et des services
- Gestion des risques liés à la chaîne d'approvisionnement

La procédure d'évaluation consiste en un ensemble d'objectifs d'évaluation comportant chacun un ensemble connexe des méthodes et des objets d'évaluation potentiels. Les procédures d'évaluation mentionnées à la [section 3](#) sont tirées de l'ITSP.10.033-02. Les évaluations des exigences de sécurité comprennent plusieurs éléments clés :

- les **objets d'évaluation** définissent les éléments particuliers qui sont évalués dans le cadre d'une activité ou d'un contrôle donné et font mention des spécifications, des mécanismes, des procédures et des individus;
- les **spécifications** sont les artefacts basés sur le document, qui sont associés à une activité ou à un contrôle courant ou propre au système. Ces artefacts comprennent ce qui suit :
 - les stratégies;
 - les procédures;
 - les plans;
 - les exigences de sécurité et de protection de la vie privée du système;
 - les spécifications fonctionnelles;
 - les conceptions fonctionnelles;
- les **mécanismes** correspondent au matériel, aux logiciels ou aux micrologiciels particuliers, dont les dispositifs de protection physique, qui composent les protections et les contremesures employées dans un système ou dans une activité ou un contrôle courant;
- les **procédures** sont des mesures de protection particulières qui prennent en charge un système ou une activité ou un contrôle commun exigeant l'intervention d'individus, par exemple :
 - effectuer les étapes nécessaires pour sauvegarder un système;
 - surveiller le trafic d'un réseau;
 - exécuter un plan d'urgence;
- les **méthodes d'évaluation** définissent la nature des actions menées par les contrôleuses et contrôleurs et comprennent ce qui suit :
 - **examen** : processus qui consiste à vérifier, à inspecter, à observer, à étudier ou à analyser un objet d'évaluation ou plus (à savoir, les spécifications, les mécanismes ou les procédures) afin de faciliter la compréhension de la contrôleuse ou du contrôleur, d'obtenir plus de clarifications ou de rassembler des preuves;
 - **entrevue** : processus qui consiste à tenir des discussions avec les personnes ou les groupes de personnes d'une organisation afin de faciliter la compréhension de la contrôleuse ou du contrôleur, d'obtenir plus de clarifications ou de rassembler des preuves;

- **test** : processus qui consiste à réaliser un objet d'évaluation ou plus (à savoir, des procédures ou des mécanismes) conformément aux conditions définies pour comparer l'état actuel de l'objet à l'état voulu ou au comportement attendu de l'objet;
- les méthodes d'évaluation ont un ensemble d'**attributs** connexes – portée et profondeur – qui aident à définir le niveau d'efforts nécessaire à l'évaluation. Les attributs sont de nature hiérarchique et fournissent les moyens pour définir la portée, la profondeur et la rigueur de l'évaluation pour les assurances accrues dont certains systèmes pourraient avoir besoin :
 - l'attribut de la profondeur traite de la rigueur et du niveau de détail exigés par les efforts d'évaluation;
 - l'attribut de la portée traite de l'ampleur des efforts d'évaluation, comme le nombre et les types de spécifications, de mécanismes et de procédures à examiner ou à tester, ainsi que les personnes qui prendront part à une entrevue;
- le **niveau d'effort** de l'évaluation est principalement déterminé par l'évaluation des risques d'atteinte à la vie privée ou la catégorisation de la sécurité du système ou de l'activité ou du contrôle commun à évaluer conformément à ce qui est mentionné dans le document *Activités organisationnelles de gestion des risques pour la cybersécurité et la vie privée* (ITSP.10.036). Les valeurs de ces attributs vont d'un niveau d'assurance de la sécurité (NAS) 1 à un NAS 5 (les NAS sont définis dans l'ITSP.10.037, *Activités de gestion des risques pour la cybersécurité et la vie privée tout au long du cycle de vie des systèmes*);
- les valeurs d'attribut appropriées pour une méthode d'évaluation particulière sont basées sur les exigences relatives à l'assurance précisées par l'organisation et sont une composante importante de la protection de l'information en fonction du risque – ce qu'on appelle la **gestion des risques**.

Figure 1 : Structure et contenu d'une procédure d'évaluation

03.01.06 Droit d'accès minimal – Comptes privilégiés	Nom de l'exigence de sécurité
ODP:	ODP de l'exigence de sécurité
A.03.01.06.ODP: définir le personnel ou les rôles dont les comptes privilégiés devraient être restreints sur le système	
Confirmer l'exécution des actions suivantes:	Énoncé de détermination multipartite
A.03.01.06.A: limiter les comptes privilégiés sur le système à < A.03.01.06.ODP: personnel ou rôles>	
A.03.01.06.B: exiger que les utilisatrices et utilisateurs (ou rôles) de comptes privilégiés qui ont accès aux fonctions ou à l'information non liées à la sécurité utilisent des comptes non privilégiés	
A.03.01.06.C: exiger que les opérations administratives ou de superutilisatrices ou superutilisateurs soient réalisées à partir d'une station de travail physique dédiée à ces tâches précises et isolée des autres fonctions et réseau	
Méthodes et objets d'évaluation potentiels:	
Examen	
[Sélection parmi les options suivantes: politique et procédures liées au contrôle d'accès; procédures liées au droit d'accès minimal; liste des comptes privilégiés générés par le système; liste des membres du personnel d'administration du système; enregistrements de vérification du système; paramètres de configuration du système; plan de sécurité du système; liste des fonctions de sécurité générées par le système ou de l'information relative à la sécurité attribuée aux comptes ou aux rôles du système; documents sur l'architecture de gestion du système; paramètres de configuration des stations de travail administratives dédiées (STAD); autres documents ou enregistrements pertinents]	
Entrevue	
[Sélection parmi les options suivantes: personnel responsable de la définition du droit d'accès minimal; personnel responsable de la sécurité de l'information; personnel responsable de l'ingénierie de la sécurité du système; architectes de la sécurité; administratrices et administrateurs de système]	

Description longue de la figure 1 :

La figure 1 présente une capture d'écran de l'exigence de sécurité 03-01-06, Droit d'accès minimal – Comptes privilégiés. La figure vise à illustrer la structure et les principaux composants d'une exigence de sécurité, comme ils s'affichent dans la publication. Trois encadrés annotés sont utilisés pour mettre en évidence des éléments particuliers de l'exigence. Le premier encadré s'affiche près de l'en-tête de l'exigence de sécurité pour indiquer son nom. Le deuxième encadré est placé près du texte « ODP : » et précise que le texte qui se trouve en dessous contient les paramètres définis par l'organisation (ODP pour Organization-Defined Parameter) associés à l'exigence. Le troisième encadré contient le texte « énoncé de détermination multipartite » et est situé près de la phrase « Confirmer l'exécution des actions suivantes : ». Le texte qui suit dresse la liste des actions ou des conditions qu'il convient d'effectuer ou de satisfaire pour que l'exigence puisse être considérée comme étant mise en œuvre.

La structure et le contenu des procédures d'évaluation comprennent les éléments suivants qui figurent à la figure 1 :

- les **énoncés de détermination** composés d'identificateurs alphanumériques. Chaque énoncé de détermination commence par la lettre « A » pour indiquer qu'il fait partie d'une procédure d'évaluation. Ceux-ci sont souvent présentés sous forme d'« énoncés de détermination multipartites », puisque plusieurs mesures doivent être prises;
- la **séquence de chiffres ou de lettres** suivante (par exemple, 03.01.01.E ou 03.01.01.F.02) précise l'identificateur de l'exigence de sécurité tirée de l'ITSP.10.171 (et l'élément de contrôle particulier s'il s'agit d'une exigence en plusieurs parties) faisant l'objet de l'évaluation;
- les **paramètres définis par l'organisation** de l'exigence de sécurité sont indiqués par les lettres « ODP » (en anglais, *Organization-Defined Parameters*). Si l'énoncé de détermination comporte plusieurs ODP, ce nombre est indiqué entre crochets (par exemple, A.03.01.08.ODP[01]);
- les **crochets** sont utilisés pour illustrer qu'une procédure d'évaluation divise une exigence en plusieurs énoncés de détermination granulaires (par exemple, A.03.01.12.A[01], A.03.01.12.A[02], A.03.01.12.A[03]);
- l'application d'une procédure d'évaluation à une exigence de sécurité donne lieu à des résultats ou à des **constatations**. Les constatations sont compilées et servent de preuves pour déterminer si l'exigence de sécurité a été satisfaite ou si elle porte toute autre mention :
 - une constatation ayant reçu la mention **satisfaite** indique que l'objectif de l'évaluation a été atteint et que cette dernière a fourni un résultat tout à fait acceptable;
 - une constatation ayant reçu une mention **autre que satisfaite** indique qu'il y a de possibles anomalies auxquelles l'organisation devra s'attaquer. Une telle mention pourrait également indiquer que la contrôlease ou le contrôleur n'a pas été en mesure d'obtenir suffisamment d'information pour en venir à la détermination nécessaire à l'énoncé de détermination.

2.2 Cas d'assurance

Afin de présenter un cas d'assurance efficace pour assurer l'efficacité des contrôles et la qualité de l'exécution des activités, il convient de compiler les preuves de diverses procédures d'assurance effectuées dans le cadre du cycle de vie des systèmes. Les preuves proviennent des contrôles et des activités de sécurité et de protection de la vie privée qui sont mis en œuvre dans le système et hérités par ce dernier (contrôles courants), ainsi que de l'évaluation de cette mise en œuvre.

Les activités d'assurance peuvent être menées à deux différents niveaux :

- elles peuvent être liées à un contrôle particulier et prendre en charge un produit ou un mécanisme de sécurité en particulier;
- elles peuvent prendre en charge le système dans son intégralité pour évaluer son développement et l'intégration des contrôles dans ce dernier.

Les activités d'assurance qui prennent en charge le développement des systèmes visent à améliorer les résultats en matière de conception, d'architecture et d'ingénierie. Les activités d'assurance que l'on désignait sous le nom « activités » dans le [Catalogue des activités d'assurance et des contrôles de sécurité et de protection de la vie privée \(ITSP.10.033\)](#) fonctionnent de la même façon.

L'évaluation d'un contrôle ou d'une activité est une procédure d'assurance. Au moment d'évaluer une activité d'assurance, tel qu'il est indiqué dans l'ITSP.10.033, il convient de mettre l'accent sur l'évaluation de la qualité de son exécution. Ce processus est décrit en détail dans l'ITSP.10.037.

Ensemble, la force et l'assurance définissent les exigences qu'il faut respecter au moment de mettre en œuvre un contrôle pour répondre à son objectif en matière de sécurité ou de protection de la vie privée.

La **force** de la sécurité ou de la protection de la vie privée est associée à la capacité potentielle du contrôle mis en œuvre de protéger la confidentialité, l'intégrité ou la disponibilité des biens. À mesure que la force augmente, l'auteur de menace doit déployer des efforts plus grands et déboursier des coûts additionnels pour contourner le contrôle mis en œuvre.

Le potentiel de protection d'un contrôle ne peut être réalisé que si ce contrôle est mis en œuvre avec une assurance adéquate.

L'**assurance** consiste en des tâches visant à accroître la confiance que l'on effectue pour s'assurer qu'un contrôle est conçu et mis en œuvre correctement et qu'il fonctionne comme prévu, ou qu'une activité d'assurance est réalisée de façon appropriée. L'assurance comprend également les tâches qui permettent de s'assurer que tous les contrôles associés à la conception, à la mise en œuvre et au fonctionnement d'un système répondent aux besoins opérationnels en matière de sécurité et de protection de la vie privée.

L'assurance est fournie par les tâches effectuées par les développeuses et développeurs des systèmes, les responsables de la mise en œuvre et de la maintenance, les exploitantes et exploitants, ainsi que les évaluatrices et évaluateurs de la sécurité et de la protection de la vie privée. L'assurance augmente lorsqu'on déploie des efforts additionnels dans la portée et la profondeur de ces tâches, puisqu'elle contribue à l'efficacité de la preuve et aux mesures de confiance. La rigueur et la profondeur suivent généralement la même trajectoire : si une augmente, cela devrait également être le cas pour l'autre.

La **robustesse** est une caractérisation de la force et de l'assurance d'un contrôle de sécurité ou de protection de la vie privée. La force est associée à la capacité potentielle du contrôle de protéger la confidentialité, l'intégrité ou la disponibilité des biens. On a attribué aux activités d'assurance décrites dans le catalogue un niveau d'assurance seulement, et non un niveau de robustesse.

Un contrôle incorpore un élément de force lorsqu'il atténue un savoir-faire en particulier. Comme les activités d'assurance ne permettent pas de contrer directement le savoir-faire, le concept de force ne s'applique pas. L'assurance d'un contrôle est liée à la mesure dans laquelle on peut avoir la certitude que le contrôle a été conçu et mis en œuvre correctement, qu'il fonctionne comme prévu et qu'il permet d'atteindre les résultats prévus en répondant aux exigences du système et de l'organisation en matière de sécurité et de protection de la vie privée.

Par exemple, un contrôle de sécurité peut être robuste du point de vue de sa conception (comme un mécanisme d'authentification multifacteur [AMF]) et ne comprendre aucune assurance (dans la mesure où il n'y a aucune évidence, comme un examen de la sécurité ou un test de la vulnérabilité visant à démontrer la qualité de sa mise en œuvre). Dans un tel cas, il aura une robustesse réelle inférieure à un contrôle similaire ayant une assurance de niveau plus élevé (comme un mécanisme ayant été validé dans le cadre d'une validation et de tests rigoureux pour confirmer sa sécurité).

Les contrôles utilisés pour protéger des biens plus sensibles ou essentiels, ou qui sont exposés à des menaces plus sérieuses, exigent généralement des solutions de sécurité et de protection de la vie privée plus robustes et une mise en œuvre offrant une plus grande assurance et des niveaux de robustesse plus élevés.

Le modèle de robustesse établit une hiérarchie basée sur les niveaux de préjudice et de menace prévus. L'ITSP.10.037 et le document [Détermination de la robustesse des contrôles de périmètre \(ITSP.80.032\)](#) fournissent de plus amples renseignements sur le modèle de robustesse.

L'évaluation de la couverture d'un contrôle permet de répondre aux questions suivantes :

- Le contrôle permet-il de protéger adéquatement les biens voulus ou les autres contrôles connexes qu'il prend en charge?
- Le contrôle est-il appliqué correctement dans l'ensemble du système?

Par exemple, si une organisation érige une clôture (un contrôle) autour de son terrain pour sécuriser les trois quarts de son périmètre, laissant un quart sans protection, la sécurité fournie par la clôture sera incomplète. Le quart non protégé mine l'efficacité des parties sécurisées et fait en sorte que tout le périmètre est vulnérable.

Une évaluation doit considérer bien plus que la seule présence d'un contrôle. Bien qu'on puisse répondre « Oui » à la question concernant l'existence du contrôle, la question cruciale est « Le contrôle offre-t-il une couverture appropriée? ». Dans ce cas, la réponse est non, puisque la couverture est insuffisante. Cet exemple illustre l'importance d'évaluer la convenance et l'efficacité de la mise en œuvre d'un contrôle.

3 Procédures

Cette section décrit les procédures d'évaluation qui sont exclusives aux exigences de sécurité définies dans l'ITSP.10.171. Les organisations qui procèdent aux évaluations des exigences de sécurité peuvent élaborer des plans d'évaluation de sécurité à partir de l'information fournie dans le cadre des procédures d'évaluation et sélectionner les méthodes et objets d'évaluation qui répondent à leurs besoins. Les organisations ont également la souplesse nécessaire pour définir le niveau de rigueur et de détail associé à l'évaluation en fonction de leurs exigences en matière d'assurance.

3.1 Contrôle d'accès

Les contrôles de la famille Contrôle d'accès permettent d'autoriser ou de refuser l'accès des utilisatrices et utilisateurs à des ressources dans le système.

03.01.01 Gestion des comptes

ODP :

A.03.01.01.ODP[01] : définir la période d'inactivité du compte avant sa désactivation

A.03.01.01.ODP[02] : définir les délais dans lesquels il convient d'informer les gestionnaires de compte, ainsi que le personnel ou les rôles définis, lorsque les comptes ne sont plus requis

A.03.01.01.ODP[03] : définir les délais dans lesquels il convient d'informer les gestionnaires de compte, ainsi que le personnel ou les rôles définis, lorsque des utilisatrices ou utilisateurs ont quitté leur emploi ou ont fait l'objet d'un transfert

A.03.01.01.ODP[04] : définir les délais dans lesquels il convient d'informer les gestionnaires de compte, ainsi que le personnel ou les rôles définis, lorsque des changements sont apportés à l'utilisation du système ou au principe du besoin de savoir

A.03.01.01.ODP[05] : définir la période d'inactivité prévue avant que les utilisatrices et utilisateurs soient tenus de se déconnecter du système

A.03.01.01.ODP[06] : définir les circonstances dans lesquelles les utilisatrices et utilisateurs sont tenus de se déconnecter du système

Confirmer l'exécution des actions suivantes :

A.03.01.01.A[01] : définir les types de comptes autorisés du système

A.03.01.01.A[02] : définir les types de comptes interdits du système

A.03.01.01.B[01] : créer les comptes du système conformément aux stratégies, aux procédures, aux préalables et aux critères de l'organisation

A.03.01.01.B[02] : activer les comptes du système conformément aux stratégies, aux procédures, aux préalables et aux critères de l'organisation

A.03.01.01.B[03] : modifier les comptes du système conformément aux stratégies, aux procédures, aux préalables et aux critères de l'organisation

A.03.01.01.B[04] : désactiver les comptes du système conformément aux stratégies, aux procédures, aux préalables et aux critères de l'organisation

A.03.01.01.B[05] : supprimer les comptes du système conformément aux stratégies, aux procédures, aux préalables et aux critères de l'organisation

A.03.01.01.C.01 : désigner les utilisatrices et utilisateurs autorisés du système

A.03.01.01.C.02 : préciser les appartenances aux groupes et aux rôles

A.03.01.01.C.03 : préciser les autorisations d'accès (par exemple, les privilèges) pour chaque compte

A.03.01.01.D.01 : autoriser l'accès au système en fonction d'une autorisation d'accès valide

A.03.01.01.D.02 : autoriser l'accès au système en fonction de l'utilisation prévue du système

A.03.01.01.E : surveiller l'utilisation des comptes du système

A.03.01.01.F.01 : désactiver les comptes du système lorsque les comptes arrivent à expiration

A.03.01.01.F.02 : désactiver les comptes du système lorsque les comptes sont inactifs pendant **<A.03.01.01.ODP[01] : délai>**

A.03.01.01.F.03 : désactiver les comptes du système lorsque les comptes ne sont plus associés à une utilisatrice ou un utilisateur, ou à une personne

A.03.01.01.F.04 : désactiver les comptes du système lorsque les comptes enfreignent la stratégie de l'organisation

A.03.01.01.F.05 : désactiver les comptes du système lorsque des risques importants liés à des individus sont découverts

A.03.01.01.G.01 : notifier les gestionnaires de comptes, ainsi que le personnel ou les rôles définis, dans les **<A.03.01.01.ODP[02] : délai>** lorsque les comptes ne sont plus requis

A.03.01.01.G.02 : notifier les gestionnaires de comptes, ainsi que le personnel ou les rôles définis, dans les **<A.03.01.01.ODP[03] : délai>** lorsque les utilisatrices ou utilisateurs quittent leur emploi ou font l'objet d'un transfert

A.03.01.01.G.03 : notifier les gestionnaires de comptes, ainsi que le personnel ou les rôles définis, dans les **<A.03.01.01.ODP[04] : délai>** lorsque des changements sont apportés à l'utilisation qu'une personne fait du système ou au principe du besoin de savoir auquel elle est sujette

A.03.01.01.H : exiger que les utilisatrices et utilisateurs se déconnectent du système après **<A.03.01.01.ODP[05] : délai>** d'inactivité prévue ou dans les circonstances suivantes : **<A.03.01.01.ODP[06] : circonstances>**

Méthodes et objets d'évaluation potentiels :

Examen

[Sélection parmi les options suivantes : politique et procédures de contrôle d'accès; stratégies et procédures de fin d'emploi ou de transfert du personnel; procédures de gestion des comptes; liste des comptes actifs du système et nom des personnes associées à chaque compte; documents sur la conception du système; liste des conditions liées à l'appartenance

à un groupe ou à un rôle; paramètres de configuration du système; notifications des départs, fins d'emploi ou transferts récents du personnel; liste des comptes désactivés du système et nom des activités d'utilisateur qui posent des risques importants pour l'organisation; enregistrements des autorisations d'accès; examens de conformité de la gestion des comptes; enregistrements de vérification et de surveillance du système; plan de sécurité du système; plan de protection de la vie privée; liste générée par le système des comptes supprimés; liste générée par le système des comptes d'urgence désactivés; liste générée par le système des comptes désactivés; autres documents et enregistrements pertinents]

Entrevue

[Sélection parmi les options suivantes : personnel responsable de la gestion de comptes; administratrices et administrateurs de système; personnel responsable de la sécurité de l'information et de la protection de la vie privée; développeuses et développeurs de système]

Test

[Sélection parmi les options suivantes : processus de gestion des comptes sur le système; mécanismes de mise en œuvre de la gestion des comptes]

Références :

Procédures d'évaluation tirées de la source : AC-02, AC-02(03), AC-02(05) et AC-02(13)

03.01.02 Application de l'accès

Confirmer l'exécution des actions suivantes :

A.03.01.02[01] : appliquer les autorisations approuvées pour l'accès logique à l'information désignée conformément aux stratégies de contrôle d'accès applicables

A.03.01.02[02] : appliquer les autorisations approuvées pour l'accès logique aux ressources du système conformément aux stratégies de contrôle d'accès applicables

Méthodes et objets d'évaluation potentiels :

Examen

[Sélection parmi les options suivantes : politique et procédures de contrôle d'accès; procédures d'application de l'accès; documents sur la conception du système; paramètres de configuration du système; liste des autorisations approuvées (par exemple, privilèges utilisateur); enregistrements de vérification du système; plan de sécurité du système; autres documents ou enregistrements pertinents]

Entrevue

[Sélection parmi les options suivantes : personnel responsable de l'application de l'accès; administratrices et administrateurs de système; personnel responsable de la sécurité de l'information; développeuses et développeurs de système]

Test

[Sélection parmi les options suivantes : mécanismes de mise en œuvre de la politique de contrôle d'accès]

Références :

Procédure d'évaluation tirée de la source : AC-03

03.01.03 Application du contrôle de flux d'information**Confirmer l'exécution des actions suivantes :**

A.03.01.03[01] : appliquer les autorisations approuvées pour contrôler le flux de l'information désignée dans le système

A.03.01.03[02] : appliquer les autorisations approuvées pour contrôler le flux de l'information désignée entre des systèmes connectés

Méthodes et objets d'évaluation potentiels :**Examen**

[Sélection parmi les options suivantes : politique et procédures de contrôle d'accès; stratégies de contrôle du flux d'information; procédures d'application du contrôle de flux d'information; documents sur l'architecture et la conception de la sécurité; paramètres de configuration du système; configuration de référence du système; enregistrements de vérification du système; liste des autorisations du flux d'information; plan de sécurité du système; plan de protection de la vie privée; autres documents ou enregistrements pertinents]

Entrevue

[Sélection parmi les options suivantes : administratrices et administrateurs de système; personnel responsable de l'architecture de sécurité et de protection de la vie privée; personnel responsable de la sécurité de l'information et de la protection de la vie privée; développeuses et développeurs de système]

Test

[Sélection parmi les options suivantes : mécanismes de mise en œuvre de la stratégie d'application du flux d'information]

Références :

Procédure d'évaluation tirée de la source : AC-04

03.01.04 Séparation des tâches**Confirmer l'exécution des actions suivantes :**

A.03.01.04.A : établir les tâches assumées par le personnel nécessitant une séparation

A.03.01.04.B : définir les autorisations d'accès au système afin d'appuyer la séparation des tâches

Méthodes et objets d'évaluation potentiels :**Examen**

[Sélection parmi les options suivantes : politique et procédures de contrôle d'accès; procédures pour la séparation des tâches et la division des responsabilités; paramètres de configuration du système; enregistrements de vérification du

système; autorisations d'accès au système; liste des divisions des responsabilités et de la séparation des tâches; plan de sécurité du système; autres documents ou enregistrements pertinents]

Entrevue

[Sélection parmi les options suivantes : personnel responsable de la définition de la séparation des tâches et de la division des responsabilités; personnel responsable de la sécurité de l'information; administratrices et administrateurs de système]

Test

[Sélection parmi les options suivantes : mécanismes de mise en œuvre de la stratégie sur la séparation des tâches]

Références :

Procédure d'évaluation tirée de la source : AC-05

03.01.05 Droit d'accès minimal

ODP :

A.03.01.05.ODP[01] : définir les fonctions de sécurité pour un accès autorisé

A.03.01.05.ODP[02] : définir l'information pertinente en matière de sécurité pour un accès autorisé

A.03.01.05.ODP[03] : définir la fréquence à laquelle il convient d'examiner les droits d'accès attribués aux rôles ou aux classes d'utilisateur

Confirmer l'exécution des actions suivantes :

A.03.01.05.A : autoriser les accès au système pour les utilisatrices et utilisateurs (ou les processus exécutés en leur nom) qui sont nécessaires pour accomplir les tâches organisationnelles assignées

A.03.01.05.B[01] : autoriser l'accès à **<A.03.01.05.ODP[01] : fonctions de sécurité>**

A.03.01.05.B[02] : autoriser l'accès à **<A.03.01.05.ODP[02] : information pertinente en matière de sécurité>**

A.03.01.05.C : examiner les privilèges attribués aux rôles ou aux classes d'utilisateur tous les **<A.03.01.05.ODP[03] : fréquence>** afin de valider la nécessité de détenir ces privilèges

A.03.01.05.D : réattribuer ou retirer les privilèges, au besoin

Méthodes et objets d'évaluation potentiels :

Examen

[Sélection parmi les options suivantes : politique et procédures liées au contrôle d'accès; procédures liées au droit d'accès minimal; liste des autorisations d'accès attribuées (privilèges d'utilisateur); paramètres de configuration du système; enregistrements de vérification du système; liste des fonctions de sécurité (mises en œuvre dans le matériel, les logiciels et les micrologiciels); information relative à la sécurité dont l'accès exige une autorisation explicite; liste des rôles ou des classes d'utilisateurs générés par le système et des privilèges attribués; examens de validation des privilèges attribués aux rôles ou aux classes d'utilisateurs; enregistrements du retrait ou de la réaffectation des privilèges attribués aux rôles ou aux

classes d'utilisateurs; plan de sécurité du système; documents sur la conception du système; autres documents ou enregistrements pertinents]

Entrevue

[Sélection parmi les options suivantes : personnel responsable de la définition du droit d'accès minimal; personnel responsable de la sécurité de l'information; administratrices et administrateurs de système]

Test

[Sélection parmi les options suivantes : mécanismes de mise en œuvre des fonctions de droit d'accès minimal; mécanismes de mise en œuvre de l'examen des privilèges d'utilisateur]

Références :

Procédures d'évaluation tirées de la source : AC-06, AC-06(01), AC-06(07) et AU-09(04)

03.01.06 Droit d'accès minimal – Comptes privilégiés

ODP :

A.03.01.06.ODP : définir le personnel ou les rôles dont les comptes privilégiés devraient être restreints sur le système

Confirmer l'exécution des actions suivantes :

A.03.01.06.A : limiter les comptes privilégiés sur le système à **<A.03.01.06.ODP : personnel ou rôles>**

A.03.01.06.B : exiger que les utilisatrices et utilisateurs (ou rôles) de comptes privilégiés qui ont accès aux fonctions ou à l'information non liées à la sécurité utilisent des comptes non privilégiés

A.03.01.06.C : exiger que les opérations administratives ou de superutilisatrices ou superutilisateurs soient réalisées à partir d'une station de travail physique dédiée à ces tâches précises et isolée des autres fonctions et réseau

Méthodes et objets d'évaluation potentiels :

Examen

[Sélection parmi les options suivantes : politique et procédures liées au contrôle d'accès; procédures liées au droit d'accès minimal; liste des comptes privilégiés générés par le système; liste des membres du personnel d'administration du système; enregistrements de vérification du système; paramètres de configuration du système; plan de sécurité du système; liste des fonctions de sécurité générées par le système ou de l'information relative à la sécurité attribuée aux comptes ou aux rôles du système; documents sur l'architecture de gestion du système; paramètres de configuration des stations de travail administratives dédiées (STAD); autres documents ou enregistrements pertinents]

Entrevue

[Sélection parmi les options suivantes : personnel responsable de la définition du droit d'accès minimal; personnel responsable de la sécurité de l'information; personnel responsable de l'ingénierie de la sécurité du système; architectes de la sécurité; administratrices et administrateurs de système]

Test

[Sélection parmi les options suivantes : mécanismes de mise en œuvre des fonctions de droit d'accès minimal; tests d'intrusion sur la STAD]

Références :

Procédures d'évaluation tirées de la source : AC-06(02), AC-06(05) et SI-400

03.01.07 Droit d'accès minimal – Fonctions privilégiées**Confirmer l'exécution des actions suivantes :**

A.03.01.07.A : empêcher les utilisatrices ou utilisateurs non privilégiés d'exécuter des fonctions privilégiées

A.03.01.07.B : journaliser l'exécution des fonctions privilégiées

Méthodes et objets d'évaluation potentiels :**Examen**

[Sélection parmi les options suivantes : politique et procédures de contrôle d'accès; procédures liées au droit d'accès minimal; documents sur la conception du système; paramètres de configuration du système; enregistrements de vérification du système; liste des événements vérifiés; liste des fonctions privilégiées à vérifier et à associer aux affectations de comptes d'utilisateur; plan de sécurité du système; autres documents ou enregistrements pertinents]

Entrevue

[Sélection parmi les options suivantes : personnel responsable de l'examen du droit d'accès minimal; personnel responsable de la sécurité de l'information; développeuses et développeurs de système; administratrices et administrateurs de système]

Test

[Sélection parmi les options suivantes : mécanismes de vérification de l'exécution des fonctions du droit d'accès minimal; mécanismes de mise en œuvre des fonctions du droit d'accès minimal pour les utilisatrices et utilisateurs non privilégiés]

Références :

Procédures d'évaluation tirées de la source : AC-06(09) et AC-06(10)

03.01.08 Tentatives d'ouverture de session infructueuses**ODP :**

A.03.01.08.ODP[01] : définir le nombre de tentatives d'ouverture de session non valides consécutives par l'utilisatrice ou utilisateur sur une période déterminée

A.03.01.08.ODP[02] : définir la période durant laquelle il convient de limiter le nombre de tentatives d'ouverture de session non valides consécutives par l'utilisatrice ou utilisateur

A.03.01.08.ODP[03] : sélection d'une ou plusieurs options parmi les valeurs de paramètres suivantes : {verrouiller automatiquement le compte ou le nœud pendant <**A.03.01.08.ODP[04]** : délai>; verrouiller automatiquement le compte et le

nœud jusqu'à ce qu'une administratrice ou un administrateur le libère; retarder automatiquement la prochaine invite d'ouverture de session; aviser automatiquement l'administratrice ou administrateur de système; prendre automatiquement une autre mesure}

A.03.01.08.ODP[04] : définir la période durant laquelle il convient de verrouiller un compte ou un nœud (le cas échéant)

Confirmer l'exécution des actions suivantes :

A.03.01.08.A : appliquer une limite de **<A.03.01.08.ODP[01] : nombre>** tentatives d'ouverture de session non valides consécutives par l'utilisatrice ou utilisateur sur une période de **<A.03.01.08.ODP[02] : délais>**

A.03.01.08.B : appliquer **<A.03.01.08.ODP[03] : valeurs de paramètres sélectionnées>** lorsque le nombre maximal de tentatives d'ouverture de session infructueuses est dépassé

Méthodes et objets d'évaluation potentiels :

Examen

[Sélection parmi les options suivantes : politique et procédures de contrôle d'accès; procédures liées aux tentatives d'ouverture de session infructueuses; documents sur la conception du système; enregistrement de vérification du système; paramètres de configuration du système; plan de sécurité du système; autres documents et enregistrements pertinents]

Entrevue

[Sélection parmi les options suivantes : personnel responsable de la sécurité de l'information; développeuses et développeurs de système; administratrices et administrateurs de système]

Test

[Sélection parmi les options suivantes : mécanismes de mise en œuvre de la stratégie de contrôle d'accès pour les tentatives d'ouverture de session infructueuses]

Références :

Procédure d'évaluation tirée de la source : AC-07

03.01.09 Avis d'utilisation système

Confirmer l'exécution des actions suivantes :

A.03.01.09 : afficher un message d'avis d'utilisation du système qui comprend des énoncés de protection de la vie privée et de sécurité qui sont conformes aux règles liées à l'information désignée applicables, avant d'accorder l'accès au système

Méthodes et objets d'évaluation potentiels :

Examen

[Sélection parmi les options suivantes : politique et procédures de contrôle d'accès; stratégies de sécurité et de protection de la vie privée, procédures relatives aux avis d'utilisation système; approbation documentée des avis d'utilisation système; enregistrements de vérification du système; attestation des utilisatrices et utilisateurs des avis d'utilisation système; documents sur la conception du système; paramètres de configuration du système; avis d'utilisation système; plan de

sécurité du système; plan de protection de la vie privée; évaluation des facteurs relatifs à la vie privée (EFVP); rapport d'évaluation des facteurs relatifs à la vie privée; autres documents ou enregistrements pertinents]

Entrevue

[Sélection parmi les options suivantes : personnel responsable de la sécurité de l'information et de la protection de la vie privée; conseillères et conseillers juridiques; développeuses et développeurs de système; administratrices et administrateurs de système]

Test

[Sélection parmi les options suivantes : mécanismes de mise en œuvre des avis d'utilisation système]

Références :

Procédure d'évaluation tirée de la source : AC-08

03.01.10 Verrouillage d'appareil

ODP :

A.03.01.10.ODP[01] : sélection d'une ou plusieurs options parmi les valeurs de paramètres suivantes : {procéder au verrouillage de l'appareil après <**A.03.01.10.ODP[02]** : délai> d'inactivité; exiger que l'utilisatrice ou utilisateur procède à un verrouillage d'appareil avant de laisser le système sans surveillance}

A.03.01.10.ODP[02] : définir le délai d'inactivité après lequel il convient de procéder à un verrouillage d'appareil (le cas échéant)

Confirmer l'exécution des actions suivantes :

A.03.01.10.A : prévenir l'accès au système en <**A.03.01.10.ODP[01]**: valeurs de paramètres sélectionnées>

A.03.01.10.B : préserver le verrouillage d'appareil jusqu'à ce que l'utilisatrice ou utilisateur rétablisse l'accès au moyen des procédures d'identification et d'authentification établies

A.03.01.10.C : masquer, au moyen d'un verrouillage d'appareil, l'information auparavant visible à l'écran en utilisant une image visible

Méthodes et objets d'évaluation potentiels :

Examen

[Sélection parmi les options suivantes : politique et procédures de contrôle d'accès; procédures liées au verrouillage de la session, à l'identification et à l'authentification; documents sur la conception du système; paramètres de configuration du système; écran d'affichage avec activation du verrouillage de session; plan de sécurité du système; autres documents et enregistrements pertinents]

Entrevue

[Sélection parmi les options suivantes : personnel responsable de la sécurité de l'information; développeuses et développeurs de système; administratrices et administrateurs de système]

Test

[Sélection parmi les options suivantes : mécanismes de mise en œuvre de la stratégie de contrôle d'accès pour le verrouillage de session; mécanismes de verrouillage de session]

Références :

Procédures d'évaluation tirées de la source : AC-11 et AC-11(01)

03.01.11 Fin de session**ODP :**

A.03.01.11.ODP : définir les conditions ou les événements déclencheurs qui exigent l'interruption de la session

Confirmer l'exécution des actions suivantes :

A.03.01.11 : mettre automatiquement fin à une session utilisateur après **<A.03.01.11.ODP : conditions ou événements déclencheurs>**

Méthodes et objets d'évaluation potentiels :**Examen**

[Sélection parmi les options suivantes : politique et procédures de contrôle d'accès; procédures d'interruption de session; documents sur la conception du système; paramètres de configuration du système; liste des conditions ou des événements déclencheurs exigeant l'interruption de la session; enregistrements de vérification du système; plan de sécurité du système; autres documents ou enregistrements pertinents]

Entrevue

[Sélection parmi les options suivantes : personnel responsable de la sécurité de l'information; développeuses et développeurs de système; administratrices et administrateurs de système]

Test

[Sélection parmi les options suivantes : mécanismes automatisés pour mettre fin à la session utilisateur]

Références :

Procédure d'évaluation tirée de la source : AC-12

03.01.12 Accès à distance**Confirmer l'exécution des actions suivantes :**

A.03.01.12.A[01] : définir les types d'accès à distance au système pouvant être autorisé

A.03.01.12.A[02] : établir les restrictions d'utilisation pour chaque type d'accès à distance au système pouvant être autorisé

A.03.01.12.A[03] : établir les exigences en matière de configuration pour chaque type d'accès à distance au système pouvant être autorisé

A.03.01.12.A[04] : établir les exigences en matière de connexion pour chaque type d'accès à distance au système pouvant être autorisé

A.03.01.12.B : autoriser chaque type d'accès à distance au système avant d'établir une telle connexion

A.03.01.12.C[01] : acheminer l'accès à distance au système au moyen de points de contrôle d'accès autorisés

A.03.01.12.C[02] : acheminer l'accès à distance au système au moyen de points de contrôles d'accès gérés

A.03.01.12.D[01] : autoriser l'exécution à distance de commandes privilégiées

A.03.01.12.D[02] : autoriser l'accès à distance à l'information pertinente en matière de sécurité

Méthodes et objets d'évaluation potentiels :

Examen

[Sélection parmi les options suivantes : politique et procédures de contrôle d'accès; procédures liées à l'accès à distance aux systèmes; exigences en matière de configuration et de connexion pour l'accès à distance aux systèmes; plan de gestion des configurations; paramètres de configuration du système; autorisations de l'accès à distance; enregistrements de vérification du système; documents sur la conception du système; procédures liées à l'accès à distance au système; enregistrements de surveillance des systèmes; liste des points de contrôle d'accès réseau gérés; plan de sécurité du système; autres documents ou enregistrements pertinents]

Entrevue

[Sélection parmi les options suivantes : personnel responsable de la gestion des connexions d'accès à distance; personnel responsable de la sécurité de l'information; administratrices et administrateurs de système]

Test

[Sélection parmi les options suivantes : mécanismes de surveillance et de contrôle des méthodes d'accès à distance; mécanismes d'acheminement des accès à distance au moyen de points de contrôle d'accès gérés; capacité de gestion de l'accès à distance au système]

Références :

Procédures d'évaluation tirées de la source : AC-17, AC-17(03) et AC-17(04)

03.01.13 Non affecté

Retiré par le NIST.

03.01.14 Non affecté

Retiré par le NIST.

03.01.15 Non affecté

Retiré par le NIST.

03.01.16 Accès sans fil

Confirmer l'exécution des actions suivantes :

A.03.01.16.A[01] : définir chaque type d'accès sans fil au système

A.03.01.16.A[02] : établir les restrictions d'utilisation pour chaque type d'accès sans fil au système

A.03.01.16.A[03] : établir les exigences en matière de configuration pour chaque type d'accès sans fil au système

A.03.01.16.A[04] : établir les exigences en matière de connexion pour chaque type d'accès sans fil au système

A.03.01.16.B : autoriser chaque type d'accès sans fil au système avant d'utiliser de telles connexions

A.03.01.16.C : désactiver les capacités de réseautage sans fil intégrées aux composants du système avant leur remise et leur déploiement

A.03.01.16.D[01] : protéger l'accès sans fil au système au moyen de l'authentification

A.03.01.16.D[02] : protéger l'accès sans fil au système au moyen du chiffrement

Méthodes et objets d'évaluation potentiels :

Examen

[Sélection parmi les options suivantes : politique et procédures de contrôle d'accès; procédures liées à l'accès sans fil aux systèmes; exigences en matière de configuration et de connexion pour l'accès sans fil aux systèmes; plan de gestion des configurations; paramètres de configuration du système; autorisations de l'accès sans fil; enregistrements de vérification du système; documents sur la conception du système; plan de sécurité du système; autres documents ou enregistrements pertinents]

Entrevue

[Sélection parmi les options suivantes : personnel responsable de la gestion des connexions d'accès sans fil; personnel responsable de la sécurité de l'information; développeuses et développeurs de système; administratrices et administrateurs de système]

Test

[Sélection parmi les options suivantes : capacité de gestion de l'accès sans fil au système; mécanismes de mise en œuvre des mesures de protection de l'accès sans fil au système; mécanismes de gestion de la désactivation des capacités de réseautage sans fil]

Références :

Procédures d'évaluation tirées de la source : AC-18, AC-18(01) et AC-18(03)

03.01.17 Non affecté

Retiré par le NIST.

03.01.18 Contrôle d'accès pour les appareils mobiles

Confirmer l'exécution des actions suivantes :

A.03.01.18.A[01] : établir des restrictions d'utilisation pour les appareils mobiles

A.03.01.18.A[02] : établir les exigences en matière de configuration pour les appareils mobiles

A.03.01.18.A[03] : établir les exigences en matière de connexion pour les appareils mobiles

A.03.01.18.B : autoriser la connexion des appareils mobiles au système

A.03.01.18.C : mettre en œuvre un chiffrement complet des appareils ou un chiffrement des contenants afin de protéger la confidentialité de l'information désignée sur les appareils mobiles

Méthodes et objets d'évaluation potentiels :

Examen

[Sélection parmi les options suivantes : politique et procédures du contrôle d'accès; procédures liées au contrôle d'accès des appareils mobiles; documents sur la conception du système; plan de gestion des configurations; paramètres de configuration du système; autorisation des connexions des appareils mobiles aux systèmes organisationnels; enregistrements de vérification du système; mécanismes de chiffrement et documents de configuration connexes; plan de sécurité du système; autres documents ou enregistrements pertinents]

Entrevue

[Sélection parmi les options suivantes : personnel responsable du contrôle d'accès aux appareils mobiles; personnel utilisant des appareils mobiles pour accéder aux systèmes organisationnels; personnel responsable de la sécurité de l'information; administratrices et administrateurs de système]

Test

[Sélection parmi les options suivantes : capacité de contrôle d'accès pour les connexions des appareils mobiles aux systèmes organisationnels; mécanismes de chiffrement pour la protection de la confidentialité de l'information désignée sur les appareils mobiles; configurations d'appareils mobiles]

Références :

Procédures d'évaluation tirées de la source : AC-19 et AC-19(05)

03.01.19 Non affecté

Retiré par le NIST.

03.01.20 Utilisation de systèmes externes

ODP :

A.03.01.20.ODP : établir les exigences de sécurité à respecter sur les systèmes externes avant de permettre aux personnes autorisées de les utiliser ou d'y accéder

Confirmer l'exécution des actions suivantes :

A.03.01.20.A : interdire l'utilisation des systèmes externes, à moins qu'ils ne soient explicitement autorisés

A.03.01.20.B : respecter les exigences de sécurité suivantes sur les systèmes externes avant de permettre aux personnes autorisées de les utiliser ou d'y accéder : **<A.03.01.20.ODP : exigences de sécurité>**

A.03.01.20.C.01 : autoriser les personnes à utiliser des systèmes externes pour accéder au système de l'organisation ou pour traiter, stocker ou transmettre de l'information désignée après avoir vérifié que les exigences de sécurité sur les systèmes externes indiquées dans les plans de sécurité du système de l'organisation ont été respectées

A.03.01.20.C.02 : autoriser les personnes à utiliser des systèmes externes pour accéder au système de l'organisation ou pour traiter, stocker ou transmettre de l'information désignée après avoir conservé les ententes approuvées de connexion au système ou de traitement avec les entités organisationnelles qui hébergent les systèmes externes

A.03.01.20.D : restreindre l'utilisation de dispositifs de stockage portatifs contrôlés par l'organisation aux personnes autorisées sur les systèmes externes

Méthodes et objets d'évaluation potentiels :**Examen**

[Sélection à partir des options suivantes : politique et procédures de contrôle d'accès; procédures d'utilisation de systèmes externes; conditions générales d'utilisation des systèmes externes; exigences de sécurité des systèmes externes; liste des types d'applications accessibles à partir de systèmes externes; paramètres de configuration du système; plan de sécurité du système; autres documents et enregistrements pertinents]

Entrevue

[Sélection à partir des options suivantes : personnel responsable de la définition des conditions et des exigences de sécurité pour l'utilisation des systèmes externes; personnel responsable de la sécurité de l'information; administratrices et administrateurs de système]

Test

[Sélection parmi les options suivantes : mécanismes de mise en œuvre et d'application des conditions et des exigences de sécurité pour l'utilisation de systèmes externes]

Références :

Procédures d'évaluation tirées de la source : AC-20, AC-20(01) et AC-20(02)

03.01.21 Non affecté

Retiré par le NIST.

03.01.22 Contenu accessible au public

Confirmer l'exécution des actions suivantes :

A.03.01.22.A : former les personnes autorisées pour s'assurer que l'information accessible au public ne contient aucune information désignée

A.03.01.22.B[01] : examiner le contenu des systèmes à accès public pour relever l'information désignée

A.03.01.22.B[02] : supprimer l'information désignée découverte des systèmes à accès public, le cas échéant

Méthodes et objets d'évaluation potentiels :

Examen

[Sélection parmi les options suivantes : politique et procédures de contrôle d'accès; procédures pour le contenu accessible au public; liste des utilisatrices et utilisateurs autorisés à publier du contenu accessible au public sur des systèmes de l'organisation; documents ou matériel de formation; enregistrements des vérifications d'information accessible au public; enregistrements des réponses à l'information désignée découverte sur des sites Web publics; journaux de vérification du système; enregistrements de formation de sensibilisation à la sécurité; plan de sécurité du système; autres documents ou enregistrements pertinents]

Entrevue

[Sélection parmi les options suivantes : personnel responsable de la gestion de l'information accessible au public publiée sur des systèmes de l'organisation; personnel responsable de la sécurité de l'information]

Test

[Sélection parmi les options suivantes : mécanismes de mise en œuvre de la gestion du contenu accessible au public]

Références :

Procédure d'évaluation tirée de la source : AC-22

3.2 Sensibilisation et formation

Les contrôles de la famille Sensibilisation et formation concernent la sensibilisation des utilisatrices et utilisateurs à la sécurité du système.

03.02.01 Formation et sensibilisation en matière de sécurité

ODP :

A.03.02.01.ODP[01] : définir la fréquence à laquelle il convient de fournir une formation sur la sécurité aux utilisatrices et utilisateurs du système après la formation initiale

A.03.02.01.ODP[02] : définir les événements qui exigent que les utilisatrices et utilisateurs du système prennent part à une formation sur la sécurité

A.03.02.01.ODP[03] : définir la fréquence à laquelle il convient de mettre à jour la formation sur la sécurité aux utilisatrices et utilisateurs du système

A.03.02.01.ODP[04] : définir les événements qui exigent la mise à jour du contenu de la formation sur la sécurité

Confirmer l'exécution des actions suivantes :

A.03.02.01.A.01[01] : fournir une formation sur la sécurité aux utilisatrices et utilisateurs du système suivant la formation initiale des nouvelles utilisatrices et nouveaux utilisateurs

A.03.02.01.A.01[02] : fournir une formation sur la sécurité aux utilisatrices et utilisateurs du système tous les **<A.03.02.01.ODP[01] : fréquence>** suivant la formation initiale

A.03.02.01.A.02 : fournir une formation sur la sécurité aux utilisatrices et utilisateurs du système lorsque des changements apportés au système l'exigent ou à la suite de **<A.03.02.01.ODP[02] : événements>**

A.03.02.01.A.03[01] : fournir une formation sur la sécurité aux utilisatrices et utilisateurs du système pour que le personnel sache reconnaître les indicateurs de menace interne

A.03.02.01.A.03[02] : fournir une formation sur la sécurité aux utilisatrices et utilisateurs du système pour que le personnel sache signaler les indicateurs de menace interne

A.03.02.01.A.03[03] : fournir une formation sur la sécurité aux utilisatrices et utilisateurs du système pour que le personnel sache reconnaître les indicateurs de piratage psychologique

A.03.02.01.A.03[04] : fournir une formation sur la sécurité aux utilisatrices et utilisateurs du système pour que le personnel sache signaler les indicateurs de piratage psychologique

A.03.02.01.A.03[05] : fournir une formation sur la sécurité aux utilisatrices et utilisateurs du système pour que le personnel sache reconnaître les indicateurs d'exploration de données dans les médias sociaux

A.03.02.01.A.03[06] : fournir une formation sur la sécurité aux utilisatrices et utilisateurs du système pour que le personnel sache signaler les indicateurs d'exploration de données dans les médias sociaux

A.03.02.01.B[01] : mettre à jour le contenu de la formation sur la sécurité tous les **<A.03.02.01.ODP[03] : fréquence>**

A.03.02.01.B[02] : mettre à jour le contenu de la formation sur la sécurité à la suite de **<A.03.02.01.ODP[04] : événements>**

Méthodes et objets d'évaluation potentiels :

Examen

[Sélection parmi les options suivantes : politique et procédures de sensibilisation et de formation en matière de sécurité et de protection de la vie privée; procédures de mise en œuvre de la sensibilisation et de la formation en matière de sécurité et de protection de la vie privée; codes appropriés des règlements fédéraux; programme de sensibilisation et de formation en matière de sécurité et de protection de la vie privée; matériel de sensibilisation et de formation en matière de sécurité et de protection de la vie privée; dossiers de formation; plan de sécurité du système; plan de protection de la vie privée; autres documents ou enregistrements pertinents]

Entrevue

[Sélection parmi les options suivantes : personnel responsable de la sensibilisation et de la formation en matière de sécurité et de protection de la vie privée; personnel composé de la communauté générale d'utilisatrices et utilisateurs généraux; personnel responsable de la sécurité de l'information et de la protection de la vie privée]

Test

[Sélection parmi les options suivantes : mécanismes de gestion de la sensibilisation et de la formation en matière de sécurité de l'information et de protection de la vie privée]

Références :

Procédures d'évaluation tirées de la source : AT-02, AT-02(02) et AT-02(03)

03.02.02 Formation selon le rôle**ODP :**

A.03.02.02.ODP[01] : définir la fréquence à laquelle il convient de fournir une formation basée sur les rôles en matière de sécurité et de protection de la vie privée au personnel affecté après la formation initiale

A.03.02.02.ODP[02] : définir les événements qui exigent une formation basée sur les rôles en matière de sécurité et de protection de la vie privée

A.03.02.02.ODP[03] : définir la fréquence à laquelle il convient de mettre à jour le contenu de la formation basée sur les rôles en matière de sécurité et de protection de la vie privée

A.03.02.02.ODP[04] : définir les événements qui exigent la mise à jour du contenu de la formation basée sur les rôles en matière de sécurité et de protection de la vie privée

Confirmer l'exécution des actions suivantes :

A.03.02.02.A.01[01] : fournir une formation basée sur les rôles en matière de sécurité et de protection de la vie privée au personnel de l'organisation avant d'autoriser l'accès au système ou à l'information désignée

A.03.02.02.A.01[02] : fournir une formation basée sur les rôles en matière de sécurité et de protection de la vie privée au personnel de l'organisation avant d'exécuter les tâches attribuées

A.03.02.02.A.01[03] : fournir une formation basée sur les rôles en matière de sécurité et de protection de la vie privée au personnel de l'organisation tous les **<A.03.02.02.ODP[01] : fréquence>** après la formation initiale

A.03.02.02.A.02 : fournir une formation basée sur les rôles en matière de sécurité et de protection de la vie privée au personnel de l'organisation lorsque des changements apportés au système l'exigent ou à la suite de **<A.03.02.02.ODP[02] : événements>**

A.03.02.02.B[01] : mettre à jour le contenu de la formation basée sur les rôles en matière de sécurité et de protection de la vie privée tous les **<A.03.02.02.ODP[03] : fréquence>**

A.03.02.02.B[02] : mettre à jour le contenu de la formation basée sur les rôles en matière de sécurité et de protection de la vie privée à la suite de **<A.03.02.02.ODP[04] : événements>**

Méthodes et objets d'évaluation potentiels :**Examen**

[Sélection parmi les options suivantes : politique et procédures de sensibilisation et de formation en matière de sécurité et de protection de la vie privée; procédures pour la mise en œuvre de la formation en matière de sécurité et de protection de la vie privée; codes des règlements fédéraux; programme de formation en matière de sécurité et de protection de la vie privée; matériel de formation en matière de sécurité et de protection de la vie privée; dossiers de formation; plan de sécurité du système; autres documents ou enregistrements pertinents]

Entrevue

[Sélection parmi les options suivantes : personnel responsable de la formation basée sur les rôles en matière de sécurité et de protection de la vie privée; personnel à qui on a attribué des rôles et des responsabilités en matière de sécurité du système et de protection de la vie privée]

Test

[Sélection parmi les options suivantes : mécanismes de gestion de la sensibilisation et de la formation basée sur les rôles en matière de sécurité et de protection de la vie privée]

Références :

Procédure d'évaluation tirée de la source : AT-03

03.02.03 Non affecté

Retiré par le NIST.

3.3 Vérification et responsabilisation

Les contrôles de la famille Vérification et responsabilisation permettent de recueillir, d'analyser et de stocker les enregistrements de vérification associés aux opérations des utilisatrices et utilisateurs réalisées sur le système.

03.03.01 Journalisation d'événements**ODP :**

A.03.03.01.ODP[01] : définir les types d'événements sélectionnés pour la journalisation dans le système

A.03.03.01.ODP[02] : définir la fréquence à laquelle il convient de vérifier et de mettre à jour les types d'événements sélectionnés pour la journalisation

Confirmer l'exécution des actions suivantes :

A.03.03.01.A : préciser les types d'événements suivants pour la journalisation dans le système : **<A.03.03.01.ODP[01] : types d'événements>**

A.03.03.01.B[01] : vérifier les types d'événements sélectionnés pour la journalisation tous les <**A.03.03.01.ODP[02]** : fréquence>

A.03.03.01.B[02] : mettre à jour les types d'événements sélectionnés pour la journalisation tous les <**A.03.03.01.ODP[02]** : fréquence>

Méthodes et objets d'évaluation potentiels :

Examen

[Sélection parmi les options suivantes : politique et procédures de vérification et de responsabilisation; procédures liées aux événements vérifiables; documents sur la conception du système; paramètres de configuration du système; enregistrements de vérification du système; événements vérifiables du système; plan de sécurité du système; plan de protection de la vie privée; autres documents ou enregistrements pertinents]

Entrevue

[Sélection parmi les options suivantes : personnel responsable de la vérification et de la responsabilisation; personnel responsable de la sécurité de l'information et de la protection de la vie privée; administratrices et administrateurs de système]

Test

[Sélection parmi les options suivantes : mécanismes de mise en œuvre de la vérification du système]

Références :

Procédure d'évaluation tirée de la source : AU-02

03.03.02 Contenu des enregistrements de vérification

Confirmer l'exécution des actions suivantes :

A.03.03.02.A.01 : générer des enregistrements de vérification qui contiennent de l'information permettant d'établir le type d'événement qui s'est produit

A.03.03.02.A.02 : générer des enregistrements de vérification qui contiennent de l'information permettant d'établir le moment auquel l'événement s'est produit

A.03.03.02.A.03 : générer des enregistrements de vérification qui contiennent de l'information permettant d'établir l'endroit où l'événement s'est produit

A.03.03.02.A.04 : générer des enregistrements de vérification qui contiennent de l'information permettant d'établir la source de l'événement

A.03.03.02.A.05 : générer des enregistrements de vérification qui contiennent de l'information permettant d'établir le résultat de l'événement

A.03.03.02.A.06 : générer des enregistrements de vérification qui contiennent de l'information permettant d'établir l'identité des personnes, les sujets, les objets ou les entités associés à l'événement

A.03.03.02.B : fournir des renseignements supplémentaires pour les enregistrements de vérification, au besoin

Méthodes et objets d'évaluation potentiels :**Examen**

[Sélection parmi les options suivantes : politique et procédures de vérification et de responsabilisation; procédures liées au contenu des enregistrements de vérification; liste des événements vérifiables définis par l'organisation; documents sur la conception du système; paramètres de configuration du système; enregistrements de vérification du système; rapports d'incident du système; plan de sécurité du système; autres documents ou enregistrements pertinents]

Entrevue

[Sélection parmi les options suivantes : personnel responsable de la vérification et de la responsabilisation; personnel responsable de la sécurité de l'information; développeuses et développeurs de système; administratrices et administrateurs de système]

Test

[Sélection parmi les options suivantes : mécanismes de mise en œuvre de la vérification des événements vérifiables du système; capacité de vérification du système]

Références :

Procédures d'évaluation tirées de la source : AU-03 et AU-03(01)

03.03.03 Génération d'enregistrements de vérification**Confirmer l'exécution des actions suivantes :**

A.03.03.03.A : générer les enregistrements de vérification pour les types d'événements sélectionnés et le contenu des enregistrements de vérification indiqué dans les exigences 03.03.01 et 03.03.02

A.03.03.03.B : conserver les enregistrements de vérification pendant la période correspondant à la stratégie de conservation des dossiers

Méthodes et objets d'évaluation potentiels :**Examen**

[Sélection parmi les options suivantes : politique et procédures de vérification et de responsabilisation; procédures liées à la génération des enregistrements de vérification; documents sur la conception du système; liste des événements vérifiables; enregistrements de vérification du système; stratégie et procédures de conservation des enregistrements de vérification; période de conservation des enregistrements de vérification définie par l'organisation; archives des enregistrements de vérification; paramètres de configuration du système; plan de sécurité du système; plan de protection de la vie privée; autres documents ou enregistrements pertinents]

Entrevue

[Sélection parmi les options suivantes : personnel responsable de la génération d'enregistrements de vérification; personnel responsable de la conservation des enregistrements de vérification; personnel responsable de la sécurité de l'information et

de la protection de la vie privée; développeuses et développeurs de système; administratrices et administrateurs de système]

Test

[Sélection parmi les options suivantes : mécanismes de mise en œuvre de la capacité de génération d'enregistrements de vérification]

Références :

Procédures d'évaluation tirées de la source : AU-11 et AU-12

03.03.04 Intervention en cas d'échec du processus de journalisation des données de vérification

ODP :

A.03.03.04.ODP[01] : définir le délai pendant lequel il convient d'envoyer des alertes au personnel ou aux rôles de l'organisation en cas d'échec d'un processus de journalisation des données de vérification

A.03.03.04.ODP[02] : définir les mesures additionnelles à prendre en cas d'échec d'un processus de journalisation des données de vérification

Confirmer l'exécution des actions suivantes :

A.03.03.04.A : alerter le personnel ou les rôles de l'organisation en cas d'échec d'un processus de journalisation des données de vérification dans les **<A.03.03.04.ODP[01] : délai>**

A.03.03.04.B : prendre les mesures additionnelles suivantes : **<A.03.03.04.ODP[02]: mesures additionnelles>**

Méthodes et objets d'évaluation potentiels :

Examen

[Sélection parmi les options suivantes : politique et procédures de vérification et de responsabilisation; procédures d'intervention advenant l'échec de la vérification; documents de conception du système; paramètres de configuration du système; liste des membres du personnel à informer advenant l'échec du traitement de la vérification; enregistrements de vérification du système; plan de sécurité du système; plan de protection de la vie privée; autres documents ou enregistrements pertinents]

Entrevue

[Sélection parmi les options suivantes : personnel responsable de la vérification et de la responsabilisation; personnel responsable de la sécurité de l'information et de la protection de la vie privée; développeuses et développeurs de système; administratrices et administrateurs de système]

Test

[Sélection parmi les options suivantes : mécanismes de mise en œuvre de l'intervention advenant l'échec de la vérification]

Références :

Procédure d'évaluation tirée de la source : AU-05

03.03.05 Examen, analyse et production de rapports liés aux enregistrements de vérification

ODP :

A.03.03.05.ODP : définir la fréquence à laquelle il convient d'examiner et d'analyser les enregistrements de vérification du système

Confirmer l'exécution des actions suivantes :

A.03.03.05.A : vérifier et analyser les enregistrements de vérification du système tous les **<A.03.03.05.ODP : fréquence>** afin de repérer les indications et les répercussions potentielles d'activités inappropriées ou inhabituelles

A.03.03.05.B : signaler les résultats au personnel ou aux rôles définis de l'organisation

A.03.03.05.C[01] : analyser les enregistrements de vérification provenant de différents référentiels afin d'établir une connaissance de la situation à l'échelle de l'organisation

A.03.03.05.C[02] : mettre en corrélation les enregistrements de vérification provenant de différents référentiels afin d'établir une connaissance de la situation à l'échelle de l'organisation

Méthodes et objets d'évaluation potentiels :**Examen**

[Sélection parmi les options suivantes : politique et procédures de vérification et de responsabilisation; procédures liées à l'examen, à l'analyse et aux rapports des enregistrements de vérification; rapports sur les résultats des enregistrements de vérification; enregistrements sur les mesures prises suivant l'examen et l'analyse des enregistrements de vérification; enregistrements de vérification du système tirés de différents référentiels; plan de sécurité du système; plan de protection de la vie privée; paramètres de configuration du système; autres documents ou enregistrements pertinents]

Entrevue

[Sélection parmi les options suivantes : personnel responsable de l'examen, de l'analyse et de la production de rapports liés aux enregistrements de vérification; personnel responsable de la sécurité de l'information et de la protection de la vie privée]

Test

[Sélection parmi les options suivantes : mécanismes prenant en charge l'analyse et la mise en corrélation des enregistrements de vérification]

Références :

Procédures d'évaluation tirées de la source : AU-06 et AU-06(03)

03.03.06 Réduction des enregistrements de vérification et génération de rapports

Confirmer l'exécution des actions suivantes :

A.03.03.06.A[01] : mettre en œuvre des capacités de réduction des enregistrements de vérification et de génération de rapports pour soutenir l'examen des enregistrements de vérification

A.03.03.06.A[02] : mettre en œuvre des capacités de réduction des enregistrements de vérification et de génération de rapports pour soutenir l'analyse des enregistrements de vérification

A.03.03.06.A[03] : mettre en œuvre des capacités de réduction des enregistrements de vérification et de génération de rapports pour répondre aux exigences en matière de production de rapports

A.03.03.06.A[04] : mettre en œuvre des capacités de réduction des enregistrements de vérification et de génération de rapports pour soutenir les enquêtes après coup sur les incidents

A.03.03.06.B[01] : conserver le contenu original et la chronologie des enregistrements de vérification

A.03.03.06.B[02] : conserver le classement chronologique original des enregistrements de vérification

Méthodes et objets d'évaluation potentiels :

Examen

[Sélection parmi les options suivantes : politique et procédures de vérification et de responsabilisation; procédures liées à la réduction des enregistrements de vérification et à la génération de rapports; outils de réduction, d'examen et d'analyse des enregistrements de vérification et de génération de rapports; enregistrements de vérification du système; documents sur la conception du système; paramètres de configuration du système; plan de sécurité du système; autres documents ou enregistrements pertinents]

Entrevue

[Sélection parmi les options suivantes : personnel responsable de la réduction des enregistrements de vérification et de la génération de rapports; personnel responsable de la sécurité de l'information]

Test

[Sélection parmi les options suivantes : mécanismes de prise en charge de la capacité de réduction des enregistrements de vérification et de génération de rapports]

Références :

Procédure d'évaluation tirée de la source : AU-07

03.03.07 Horodatage

ODP :

A.03.03.07.ODP : définir la granularité de mesure du temps pour l'horodatage des enregistrements de vérification

Confirmer l'exécution des actions suivantes :

A.03.03.07.A : utiliser les horloges internes du système pour horodater les enregistrements de vérification

A.03.03.07.B[01] : consigner l'horodatage des enregistrements de vérification correspondant à **<A.03.03.07.ODP : granularité de la mesure du temps>**

A.03.03.07.B[02] : consigner l'horodatage des enregistrements de vérification utilisant le temps universel coordonné (UTC pour *Coordinated Universal Time*), un décalage fixe par rapport à l'UTC correspondant à l'heure locale, ou encore en incluant le décalage local dans les données d'horodatage

Méthodes et objets d'évaluation potentiels :

Examen

[Sélection parmi les options suivantes : politique et procédures de vérification et de responsabilisation; procédures pour la génération de l'horodatage; documents sur la conception du système; paramètres de configuration du système; enregistrements de vérification du système; plan de sécurité du système; autres documents ou enregistrements pertinents]

Entrevue

[Sélection parmi les options suivantes : personnel responsable de la sécurité de l'information; développeuses et développeurs de système; administratrices et administrateurs de système]

Test

[Sélection parmi les options suivantes : mécanismes de mise en œuvre de la génération de l'horodatage]

Références :

Procédure d'évaluation tirée de la source : AU-08

03.03.08 Protection de l'information de vérification

Confirmer l'exécution des actions suivantes :

A.03.03.08.A[01] : protéger l'information de vérification contre les accès non autorisés, les modifications et les suppressions

A.03.03.08.A[02] : protéger les outils de journalisation des enregistrements de vérification contre les accès non autorisés, les modifications et les suppressions

A.03.03.08.B : autoriser l'accès pour la gestion de la fonctionnalité de journalisation des données de vérification uniquement à un sous-ensemble d'utilisatrices et utilisateurs ou de rôles privilégiés

Méthodes et objets d'évaluation potentiels :

Examen

[Sélection parmi les options suivantes : politique et procédures de vérification et de responsabilisation; procédures de protection de l'information de vérification; paramètres de configuration du système; enregistrements de vérification du système; outils de vérification; liste générée par le système des utilisatrices ou utilisateurs privilégiés ayant accès à la gestion de la fonctionnalité de vérification; autorisations d'accès; liste de contrôle d'accès; documents sur la conception du système; plan de sécurité du système; plan de protection de la vie privée; autres documents ou enregistrements pertinents]

Entrevue

[Sélection parmi les options suivantes : personnel responsable de la vérification et de la responsabilisation; personnel responsable de la sécurité de l'information et de la protection de la vie privée; développeuses et développeurs de système; administratrices et administrateurs de système]

Test

[Sélection parmi les options suivantes : mécanismes de mise en œuvre de la protection de l'information de vérification; mécanismes de gestion de l'accès à la fonctionnalité de vérification]

Références :

Procédures d'évaluation tirées de la source : AU-09 et AU-09(04)

03.03.09 Non affecté

Retiré par le NIST.

3.4 Gestion des configurations

Les contrôles de la famille Gestion des configurations appuient la gestion et le contrôle de tous les composants du système, comme le matériel, les logiciels et les éléments de configuration.

03.04.01 Configuration de référence**ODP :**

A.03.04.01.ODP : définir la fréquence à laquelle il convient de passer en revue et de mettre à jour la configuration de référence du système

Confirmer l'exécution des actions suivantes :

A.03.04.01.A[01] : élaborer une configuration de référence du système

A.03.04.01.A[02] : tenir à jour la configuration de référence du système dans le cadre du contrôle des configurations

A.03.04.01.B[01] : passer en revue la configuration de référence du système tous les **<A.03.04.01.ODP[01] : fréquence>**

A.03.04.01.B[02] : mettre à jour la configuration de référence du système tous les **<A.03.04.01.ODP[01] : fréquence>**

A.03.04.01.B[03] : examiner la configuration de référence du système lorsque des composants de systèmes sont installés ou modifiés

A.03.04.01.B[04] : mettre à jour la configuration de référence du système lorsque des composants de systèmes sont installés ou modifiés

Méthodes et objets d'évaluation potentiels :

Examen

[Sélection parmi les options suivantes : politique et procédures de gestion des configurations; procédures liées à la configuration de référence du système; plan de gestion des configurations; documents relatifs à l'architecture d'entreprise; documents sur la conception du système; documents sur l'architecture du système; paramètres de configuration du système; inventaire des composants du système; enregistrements de contrôle des changements; plan de sécurité du système; plan de protection de la vie privée; autres documents ou enregistrements pertinents]

Entrevue

[Sélection parmi les options suivantes : personnel responsable de la gestion des configurations; personnel responsable de la sécurité de l'information et de la protection de la vie privée; administratrices et administrateurs de système]

Test

[Sélection parmi les options suivantes : processus de gestion des configurations de référence; mécanismes de prise en charge du contrôle des configurations de référence]

Références :

Procédure d'évaluation tirée de la source : CM-02

03.04.02 Paramètres de configuration**ODP :**

A.03.04.02.ODP : définir les paramètres de configuration pour le système qui cadrent avec le mode le plus rigoureux sur le plan des exigences opérationnelles

Confirmer l'exécution des actions suivantes :

A.03.04.02.A[01] : établir et documenter les paramètres de configuration suivants pour le système qui cadrent avec le mode le plus rigoureux sur le plan des exigences opérationnelles : **<A.03.04.02.ODP : paramètres de configuration>**

A.03.04.02.A[02] : mettre en œuvre les paramètres de configuration suivants pour le système : **<A.03.04.02.ODP : paramètres de configuration>**

A.03.04.02.B[01] : déterminer et documenter tout écart en ce qui a trait aux paramètres de configuration établis

A.03.04.02.B[02] : approuver tout écart en ce qui a trait aux paramètres de configuration établis

Méthodes et objets d'évaluation potentiels :**Examen**

[Sélection parmi les options suivantes : politique et procédures de gestion des configurations; procédures liées aux paramètres de configuration des systèmes; plan de gestion des configurations; documents sur la conception du système; paramètres de configuration du système; listes de vérification des configurations sécurisées communes; inventaire des composants du système; écarts approuvés par rapport aux paramètres de configuration établis avec preuves connexes; enregistrements de contrôle des changements; permissions de traitement et de conservation des données du système;

enregistrements de vérification du système; plan de sécurité du système; plan de protection de la vie privée; autres documents ou enregistrements pertinents]

Entrevue

[Sélection parmi les options suivantes : personnel responsable de la gestion des configurations liées à la sécurité; personnel responsable de la gestion des configurations liées à la protection de la vie privée; personnel responsable de la sécurité de l'information et de la protection de la vie privée; administratrices et administrateurs de système]

Test

[Sélection parmi les options suivantes : processus pour la gestion des paramètres de configuration; mécanisme de mise en œuvre, de surveillance ou de contrôle des paramètres de configuration du système; mécanismes permettant d'établir ou de documenter les écarts par rapport aux paramètres de configuration établis]

Références :

Procédure d'évaluation tirée de la source : CM-06

03.04.03 Contrôle des changements de configuration

Confirmer l'exécution des actions suivantes :

A.03.04.03.A : définir les types de changements apportés au système qui sont contrôlés par la configuration

A.03.04.03.B[01] : examiner les changements proposés au système qui sont contrôlés par la configuration en tenant compte explicitement des répercussions sur la sécurité

A.03.04.03.B[02] : approuver ou refuser les changements proposés au système qui sont contrôlés par la configuration en tenant compte explicitement des répercussions sur la sécurité

A.03.04.03.C[01] : mettre en œuvre les changements approuvés au système qui sont contrôlés par la configuration

A.03.04.03.C[02] : documenter les changements approuvés au système qui sont contrôlés par la configuration

A.03.04.03.D[01] : surveiller les activités associées aux changements contrôlés par la configuration visant le système

A.03.04.03.D[02] : examiner les activités associées aux changements contrôlés par la configuration visant le système

Méthodes et objets d'évaluation potentiels :

Examen

[Sélection parmi les options suivantes : politique et procédures de gestion des configurations; procédures liées au contrôle des changements de configuration du système; plan de gestion des configurations; documents sur l'architecture du système; paramètres de configuration; enregistrements de contrôle des changements; enregistrements de vérification du système; rapports sur l'examen et la vérification du contrôle des changements; ordres du jour, procès-verbaux et documents liés aux réunions de supervision du contrôle des changements de configuration; plan de sécurité du système; plan de protection de la vie privée; EFVP; autres documents ou enregistrements pertinents]

Entrevue

[Sélection parmi les options suivantes : personnel responsable du contrôle des changements de configuration; personnel responsable de la sécurité de l'information et de la protection de la vie privée; membres du comité de contrôle des changements ou de comités semblables; administratrices et administrateurs de système]

Test

[Sélection parmi les options suivantes : processus de contrôle des changements de configuration; mécanismes de mise en œuvre du contrôle des changements de configuration]

Références :

Procédure d'évaluation tirée de la source : CM-03

03.04.04 Analyses des répercussions**Confirmer l'exécution des actions suivantes :**

A.03.04.04.A[01] : analyser les changements visant le système pour déterminer les répercussions possibles sur la sécurité avant leur mise en œuvre

A.03.04.04.A[02] : analyser les changements visant le système pour déterminer les répercussions possibles sur la protection de la vie privée avant leur mise en œuvre

A.03.04.04.B : s'assurer que les exigences de sécurité du système continueront d'être satisfaites après la mise en œuvre des changements

Méthodes et objets d'évaluation potentiels :**Examen**

[Sélection parmi les options suivantes : politique et procédures de gestion des configurations; procédures pour l'analyse des répercussions sur la sécurité des changements visant le système; plan de gestion des configurations; documents sur l'analyse des répercussions sur la sécurité; documents sur l'analyse des répercussions sur la protection de la vie privée; EFVP; documents sur l'évaluation des risques d'atteinte à la vie privée; documents sur la conception du système; outils et résultats d'analyse; enregistrements de contrôle des changements; enregistrements de vérification du système; plan de sécurité du système; plan de protection de la vie privée; autres documents ou enregistrements pertinents]

Entrevue

[Sélection parmi les options suivantes : personnel responsable de l'analyse des répercussions sur la sécurité; personnel responsable de l'analyse des répercussions sur la protection de la vie privée; personnel responsable de la sécurité de l'information et de la protection de la vie privée; membres du comité de contrôle des changements; développeuses et développeurs de système; administratrices et administrateurs de système]

Test

[Sélection parmi les options suivantes : processus d'analyse des répercussions sur la sécurité; processus d'analyse des répercussions sur la protection de la vie privée]

Références :

Procédure d'évaluation tirée de la source : CM-04 et CM-04(02)

03.04.05 Restrictions d'accès associées aux changements**Confirmer l'exécution des actions suivantes :**

A.03.04.05[01] : définir et documenter les restrictions d'accès physiques associées aux changements apportés au système

A.03.04.05[02] : approuver les restrictions d'accès physiques associées aux changements apportés au système

A.03.04.05[03] : appliquer les restrictions d'accès physiques associées aux changements apportés au système

A.03.04.05[04] : définir et documenter les restrictions d'accès logiques associées aux changements apportés au système

A.03.04.05[05] : approuver les restrictions d'accès logiques associées aux changements apportés au système

A.03.04.05[06] : appliquer les restrictions d'accès logiques associées aux changements apportés au système

Méthodes et objets d'évaluation potentiels :**Examen**

[Sélection parmi les options suivantes : politique et procédures de gestion des configurations; procédures liées aux restrictions d'accès aux changements apportés au système; plan de gestion des configurations; documents sur la conception du système; documents sur l'architecture du système; paramètres de configuration du système; approbations d'accès logiques; approbations d'accès physiques; justificatifs d'accès; enregistrements de contrôle des changements; enregistrements de vérification du système; plan de sécurité du système; autres documents ou enregistrements]

Entrevue

[Sélection parmi les options suivantes : personnel responsable du contrôle d'accès logique; personnel responsable du contrôle d'accès physique; personnel responsable de la sécurité de l'information; administratrices et administrateurs de système]

Test

[Sélection parmi les options suivantes : processus de gestion des restrictions d'accès aux changements apportés au système; mécanismes pour le soutien, la mise en œuvre ou l'application des restrictions d'accès associées aux changements apportés au système]

Références :

Procédure d'évaluation tirée de la source : CM-05

03.04.06 Fonctionnalité minimale**ODP :**

A.03.04.06.ODP[01] : définir les fonctions à interdire ou à restreindre

A.03.04.06.ODP[02] : définir les ports à interdire ou à restreindre

A.03.04.06.ODP[03] : définir les protocoles à interdire ou à restreindre

A.03.04.06.ODP[04] : définir les connexions à interdire ou à restreindre

A.03.04.06.ODP[05] : définir les services à interdire ou à restreindre

A.03.04.06.ODP[06] : définir la fréquence à laquelle il convient d'examiner le système afin d'établir les fonctions, les ports, les protocoles, les connexions et les services non nécessaires ou non sécurisés

Confirmer l'exécution des actions suivantes :

A.03.04.06.A : configurer le système afin qu'il fournisse uniquement les capacités essentielles à la mission

A.03.04.06.B[01] : interdire ou restreindre l'utilisation des fonctions suivantes : **<A.03.04.06.ODP[01] : fonctions>**

A.03.04.06.B[02] : interdire ou restreindre l'utilisation des ports suivants : **<A.03.04.06.ODP[02] : ports>**

A.03.04.06.B[03] : interdire ou restreindre l'utilisation des protocoles suivants : **<A.03.04.06.ODP[03] : protocoles>**

A.03.04.06.B[04] : interdire ou restreindre l'utilisation des connexions suivantes : **<A.03.04.06.ODP[04] : connexions>**

A.03.04.06.B[05] : interdire ou restreindre l'utilisation des services suivants : **<A.03.04.06.ODP[05] : services>**

A.03.04.06.C : examiner le système tous les **<A.03.04.06.ODP[06] : fréquence>** afin d'établir les fonctions, les ports, les protocoles, les connexions et les services non nécessaires ou non sécurisés

A.03.04.06.D : désactiver ou retirer les fonctions, les ports, les protocoles, les connexions et les services non nécessaires ou non sécurisés

Méthodes et objets d'évaluation potentiels :

Examen

[Sélection parmi les options suivantes : politique et procédures de gestion des configurations; procédures liées au principe de fonctionnalité minimale dans le système; plan de gestion des configurations; documents sur la conception du système; paramètres de configuration du système; inventaire des composants du système; listes de vérification des configurations sécurisées communes; examens documentés des fonctions, des ports, des protocoles et des services; enregistrements de contrôle des changements; enregistrements de vérification du système; plan de sécurité du système; autres documents ou enregistrements pertinents]

Entrevue

[Sélection parmi les options suivantes : personnel responsable de la gestion des configurations; personnel responsable de l'examen des fonctions, des ports, des protocoles et des services; personnel responsable de la sécurité de l'information; développeuses et développeurs de système; administratrices et administrateurs de système]

Test

[Sélection parmi les options suivantes : processus pour l'interdiction ou la restriction des fonctions, des ports, des protocoles et des services; processus d'examen ou de désactivation des fonctions, des ports, des protocoles et des services; mécanismes pour la mise en œuvre de l'examen et de la désactivation des fonctions, des ports, des protocoles et des services; mécanismes pour la mise en œuvre des restrictions ou de l'interdiction des fonctions, des ports, des protocoles et des services]

Références :

Procédures d'évaluation tirées de la source : CM-07 et CM-07(01)

03.04.07 Non affecté

Retiré par le NIST.

03.04.08 Logiciels autorisés – Autorisation par exception**ODP :**

A.03.04.08.ODP : définir la fréquence à laquelle il convient de passer en revue et de mettre à jour la liste des programmes informatiques autorisés

Confirmer l'exécution des actions suivantes :

A.03.04.08.A : identifier les programmes informatiques pouvant être exécutés sur le système

A.03.04.08.B : mettre en œuvre une stratégie de refus par défaut, autorisation par exception pour l'exécution des programmes informatiques autorisés sur le système

A.03.04.08.C : passer en revue et mettre à jour la liste des programmes informatiques autorisés tous les **<A.03.04.08.ODP : fréquence>**

Méthodes et objets d'évaluation potentiels :**Examen**

[Sélection parmi les options suivantes : politique et procédures de gestion des configurations; procédures liées au principe de fonctionnalité minimale dans le système; plan de gestion des configurations; documents sur la conception du système; paramètres de configuration du système; liste des programmes informatiques pouvant être exécutés sur le système; inventaire des composants du système; enregistrements associés à l'examen et à la mise à jour de la liste des programmes informatiques autorisés; listes de vérification des configurations sécurisées communes; enregistrements de contrôle des changements; enregistrements de vérification du système; plan de sécurité du système; autres documents ou enregistrements pertinents]

Entrevue

[Sélection parmi les options suivantes : personnel responsable de l'identification des logiciels pouvant être exécutés sur le système; personnel responsable de la sécurité de l'information; administratrices et administrateurs de système]

Test

[Sélection parmi les options suivantes : processus lié à l'identification, à l'examen et à la mise à jour des programmes pouvant être exécutés sur le système; processus lié à la mise en œuvre de la stratégie relative aux logiciels autorisés; mécanismes de prise en charge ou de mise en œuvre de la stratégie relative aux logiciels autorisés]

Références :

Procédure d'évaluation tirée de la source : CM-07(05)

03.04.09 Non affecté

Retiré par le NIST.

03.04.10 Inventaire des composants du système

ODP :

A.03.04.10.ODP : définir la fréquence à laquelle il convient de passer en revue et de mettre à jour l'inventaire des composants du système

Confirmer l'exécution des actions suivantes :

A.03.04.10.A : élaborer et documenter un inventaire des composants du système

A.03.04.10.B[01] : passer en revue l'inventaire des composants du système tous les <**A.03.04.10.ODP : fréquence**>

A.03.04.10.B[02] : mettre à jour l'inventaire des composants du système tous les <**A.03.04.10.ODP : fréquence**>

A.03.04.10.C[01] : faire de la mise à jour de l'inventaire des composants du système une étape dans l'installation des composants

A.03.04.10.C[02] : faire de la mise à jour de l'inventaire des composants du système une étape dans le retrait des composants

A.03.04.10.C[03] : faire de la mise à jour de l'inventaire des composants du système une étape dans la mise à jour du système

Méthodes et objets d'évaluation potentiels :

Examen

[Sélection parmi les options suivantes : politique et procédures de gestion des configurations; procédures liées à l'inventaire des composants du système; plan de gestion des configurations; documents sur la conception du système; inventaire des composants du système; enregistrements d'examen et de mise à jour de l'inventaire; enregistrements d'installation des composants; enregistrements de contrôle des changements; enregistrements de retrait des composants; enregistrements de changements apportés au système; plan de sécurité du système; autres documents ou enregistrements pertinents]

Entrevue

[Sélection parmi les options suivantes : personnel responsable de la gestion de l'inventaire des composants; personnel responsable de la sécurité de l'information; administratrices et administrateurs de système]

Test

[Sélection parmi les options suivantes : processus lié à la gestion de l'inventaire des composants du système; mécanismes de prise en charge ou de mise en œuvre de l'inventaire des composants du système; processus liés à la mise à jour de l'inventaire des composants du système; mécanismes de prise en charge ou de mise en œuvre des mises à jour de l'inventaire des composants du système]

Références :

Procédures d'évaluation tirées de la source : CM-08 et CM-08(01)

03.04.11 Localisation de l'information**Confirmer l'exécution des actions suivantes :**

A.03.04.11.A[01] : établir et consigner la localisation de l'information désignée

A.03.04.11.A[02] : établir et documenter les composants du système sur lesquels l'information désignée est traitée

A.03.04.11.A[03] : établir et documenter les composants du système sur lesquels l'information désignée est stockée

A.03.04.11.B[01] : consigner les changements de la localisation du système ou des composants du système où l'information désignée est traitée

A.03.04.11.B[02] : consigner les changements de la localisation du système ou des composants du système où l'information désignée est stockée

Méthodes et objets d'évaluation potentiels :**Examen**

[Sélection parmi les options suivantes : politique et procédures de gestion des configurations; plan de gestion des configurations; procédures liées à l'identification et à la documentation de la localisation de l'information; enregistrements de vérification du système; documents sur l'architecture; documents sur la conception du système; catégorisation de la sécurité de l'information; documents sur l'inventaire des renseignements personnels; documents sur le mappage des données; enregistrements de vérification; liste des utilisatrices et utilisateurs ayant accès au système et aux composants du système; enregistrements de contrôle des changements; inventaire des composants du système; plan de sécurité du système; plan de protection de la vie privée; autres documents ou enregistrements pertinents]

Entrevue

[Sélection parmi les options suivantes : personnel responsable de la gestion de la localisation de l'information et des accès des utilisatrices et utilisateurs; personnel responsable de l'exploitation, de l'utilisation ou de la maintenance du système; personnel responsable de la sécurité de l'information et de la protection de la vie privée; développeuses et développeurs de système; administratrices et administrateurs de système]

Test

[Sélection parmi les options suivantes : processus régissant la localisation de l'information; mécanismes liés à l'application des stratégies et des méthodes relatives à l'administration de la localisation de l'information]

Références :

Procédure d'évaluation tirée de la source : CM-12

03.04.12 Configuration des systèmes et des composants pour des zones à risque élevé

ODP :

A.03.04.12.ODP[01] : définir les configurations des systèmes ou des composants de système à remettre aux personnes qui se rendent dans des endroits à risque élevé

A.03.04.12.ODP[02] : définir les exigences en matière de sécurité à appliquer aux systèmes ou aux composants de système lorsque les personnes reviennent de voyage

Confirmer l'exécution des actions suivantes :

A.03.04.12.A : remettre des systèmes ou des composants de systèmes dotés des configurations suivantes aux personnes qui voyagent dans des lieux à risque élevé : **<A.03.04.12.ODP[01] : configurations>**

A.03.04.12.B : appliquer les exigences en matière de sécurité suivantes au système ou aux composants de système lorsque les personnes reviennent de voyage : **<A.03.04.12.ODP[02] : exigences de sécurité>**

Méthodes et objets d'évaluation potentiels :

Examen

[Sélection parmi les options suivantes : politique et procédures de gestion des configurations; plan de gestion des configurations; procédures liées à la configuration de référence du système; procédures liées à l'installation et à la mise à niveau du système; inventaire des composants du système; installation ou mise à niveau des composants du système et enregistrements connexes; enregistrements de l'examen et de la mise à jour de la configuration de référence du système; paramètres de configuration du système; documents sur l'architecture du système; enregistrements de contrôle des changements; plan de sécurité du système; autres documents ou enregistrements pertinents]

Entrevue

[Sélection parmi les options suivantes : personnel responsable de la gestion des configurations; personnel responsable de la sécurité de l'information; administratrices et administrateurs de système]

Test

[Sélection parmi les options suivantes : processus liés à la gestion des configurations de référence]

Références :

Procédure d'évaluation tirée de la source : CM-02(07)

3.5 Identification et authentification

Les contrôles de la famille Identification et authentification appuient l'identification unique des utilisatrices et utilisateurs, des processus agissant au nom des utilisatrices et utilisateurs et des dispositifs. Ils appuient également l'authentification ou la vérification des identités des utilisatrices et utilisateurs, des processus et des dispositifs comme condition préalable pour accorder l'accès aux systèmes organisationnels.

03.05.01 Identification, authentification et réauthentification des utilisatrices et utilisateurs

ODP :

A.03.05.01.ODP : définir les circonstances ou les situations exigeant une réauthentification

Confirmer l'exécution des actions suivantes :

A.03.05.01.A[01] : identifier les utilisatrices et utilisateurs du système de façon unique

A.03.05.01.A[02] : authentifier les utilisatrices et utilisateurs du système

A.03.05.01.A[03] : identifier de façon unique et authentifier les utilisatrices et utilisateurs du système, puis les associer aux processus agissant en leur nom

A.03.05.01.B : réauthentifier les utilisatrices et utilisateurs lorsque **<A.03.05.01.ODP : circonstances ou situations>**

Méthodes et objets d'évaluation potentiels :

Examen

[Sélection parmi les options suivantes : politique et procédures d'identification et d'authentification; liste des circonstances ou situations exigeant une réauthentification; documents sur la conception du système; paramètres de configuration du système; enregistrements de vérification du système; liste des comptes du système; plan de sécurité du système; autres documents ou enregistrements pertinents]

Entrevue

[Sélection à partir des options suivantes : personnel responsable de l'identification et de l'authentification; personnel responsable de l'exploitation du système; personnel responsable de la gestion des comptes; développeuses et développeurs de système; personnel responsable de la sécurité de l'information; administratrices et administrateurs de système]

Test

[Sélection parmi les options suivantes : processus pour l'identification de façon unique et l'authentification des utilisatrices et utilisateurs; mécanismes de prise en charge ou de mise en œuvre des capacités d'identification et d'authentification]

Références :

Procédures d'évaluation tirées de la source : IA-02 et IA-11

03.05.02 Identification et authentification des dispositifs

ODP :

A.03.05.02.ODP : définir les dispositifs ou les types de dispositifs à identifier de façon unique et à authentifier avant d'établir une connexion

Confirmer l'exécution des actions suivantes :

A.03.05.02[01] : définir les **<A.03.05.02.ODP : dispositifs ou types de dispositifs>** de façon unique avant d'établir une connexion au système

A.03.05.02[02] : authentifier les <**A.03.05.02.ODP : dispositifs ou types de dispositifs**> avant d'établir une connexion au système

Méthodes et objets d'évaluation potentiels :

Examen

[Sélection parmi les options suivantes : politique et procédures d'identification et d'authentification; procédures d'identification et d'authentification des dispositifs; documents sur la conception du système; liste des dispositifs exigeant une identification unique et une authentification; rapports sur la connexion des dispositifs; paramètres de configuration du système; plan de sécurité du système; autres documents ou enregistrements pertinents]

Entrevue

[Sélection parmi les options suivantes : personnel responsable de l'identification et de l'authentification des dispositifs; personnel responsable de la sécurité de l'information; développeuses et développeurs de système; administratrices et administrateurs de système]

Test

[Sélection parmi les options suivantes : mécanismes de prise en charge ou de mise en œuvre des capacités d'identification et d'authentification des dispositifs]

Références :

Procédure d'évaluation tirée de la source : IA-03

03.05.03 Authentification multifacteur

Confirmer l'exécution des actions suivantes :

A.03.05.03[01] : appliquer des mécanismes d'AMF robustes pour l'accès à des comptes privilégiés

A.03.05.03[02] : appliquer des mécanismes d'AMF robustes pour l'accès à des comptes non privilégiés

Méthodes et objets d'évaluation potentiels :

Examen

[Sélection parmi les options suivantes : politique et procédures d'identification et d'authentification; documents sur la conception du système; liste des comptes du système; paramètres de configuration du système; comptes de vérification du système; plan de sécurité du système; autres documents ou enregistrements pertinents]

Entrevue

[Sélection parmi les options suivantes : personnel responsable de l'exploitation du système; personnel responsable de la gestion des comptes; personnel responsable de la sécurité de l'information; développeuses et développeurs de système; administratrices et administrateurs de système]

Test

[Sélection parmi les options suivantes : mécanismes de prise en charge ou de mise en œuvre d'une capacité d'AMF]

Références :

Procédures d'évaluation tirées de la source : IA-02(01) et IA-02(02)

03.05.04 Authentification résistant à la réinsertion**Confirmer l'exécution des actions suivantes :**

A.03.05.04[01] : mettre en œuvre des mécanismes d'authentification résistant à la réinsertion pour l'accès aux comptes privilégiés

A.03.05.04[02] : mettre en œuvre des mécanismes d'authentification résistant à la réinsertion pour l'accès aux comptes non privilégiés

Méthodes et objets d'évaluation potentiels :**Examen**

[Sélection parmi les options suivantes : politique et procédures d'identification et d'authentification; documents sur la conception du système; enregistrements de vérification du système; paramètres de configuration du système; liste des comptes privilégiés; plan de sécurité du système; autres documents ou enregistrements pertinents]

Entrevue

[Sélection parmi les options suivantes : personnel responsable de l'exploitation du système; personnel responsable de la gestion des comptes; personnel responsable de la sécurité de l'information; développeuses et développeurs de système; administratrices et administrateurs de système]

Test

[Sélection parmi les options suivantes : mécanismes de prise en charge ou de mise en œuvre des capacités d'identification et d'authentification; mécanismes de prise en charge ou de mise en œuvre de la résistance à la réinsertion]

Références :

Procédure d'évaluation tirée de la source : IA-02(08)

03.05.05 Gestion des identifiants**ODP :**

A.03.05.05.ODP[01] : définir le délai après lequel il convient de prévenir la réutilisation d'identifiant

A.03.05.05.ODP[02] : définir les caractéristiques utilisées pour identifier le statut d'une personne

Confirmer l'exécution des actions suivantes :

A.03.05.05.A : recevoir une autorisation du personnel ou des rôles de l'organisation pour attribuer un identifiant à une personne, à un groupe, à un rôle, à un service ou à un dispositif

A.03.05.05.B[01] : sélectionner un identifiant qui identifie une personne, un groupe, un rôle, un service ou un dispositif

A.03.05.05.B[02] : attribuer un identifiant qui identifie une personne, un groupe, un rôle, un service ou un dispositif

A.03.05.05.C : prévenir la réutilisation d'identifiant pendant <**A.03.05.05.ODP[01]** : délai>

A.03.05.05.D : gérer les identifiants personnels en identifiant de façon unique chaque personne à titre de
<**A.03.05.05.ODP[02]** : caractéristique>

Méthodes et objets d'évaluation potentiels :

Examen

[Sélection parmi les options suivantes : politique et procédures d'identification et d'authentification; procédures liées à la gestion des identifiants; procédures liées à la gestion des comptes; documents sur la conception du système; liste des comptes du système; liste des caractéristiques déterminant le statut de la personne; paramètres de configuration du système; liste des identifiants générée par les dispositifs de contrôle de l'accès physique; plan de sécurité du système; autres documents ou enregistrements pertinents]

Entrevue

[Sélection parmi les options suivantes : personnel responsable de la gestion des identifiants; personnel responsable de la sécurité de l'information; développeuses et développeurs de système; administratrices et administrateurs de système]

Test

[Sélection parmi les options suivantes : mécanismes de prise en charge ou de mise en œuvre de la gestion des identifiants]

Références :

Procédures d'évaluation tirées de la source : IA-04 et IA-04(04)

03.05.06 Non affecté

Retiré par le NIST.

03.05.07 Gestion des mots de passe

ODP :

A.03.05.07.ODP[01] : définir la fréquence à laquelle il convient de mettre à jour la liste des mots de passe couramment utilisés, attendus ou compromis

A.03.05.07.ODP[02] : définir la composition des mots de passe et les règles de complexité

Confirmer l'exécution des actions suivantes :

A.03.05.07.A[01] : créer une liste des mots de passe couramment utilisés, attendus ou compromis

A.03.05.07.A[02] : mettre à jour une liste des mots de passe couramment utilisés, attendus ou compromis tous les
<**A.03.05.07.ODP[01]** : fréquence>

A.03.05.07.A[03] : mettre à jour une liste des mots de passe couramment utilisés, attendus ou compromis lorsque l'on soupçonne que les mots de passe de l'organisation ont été compromis

A.03.05.07.B : vérifier que les mots de passe ne figurent pas sur la liste des mots de passe couramment utilisés, attendus ou compris lorsque les utilisatrices et utilisateurs créent ou mettent à jour des mots de passe

A.03.05.07.C : transmettre les mots de passe uniquement par des canaux protégés par chiffrement

A.03.05.07.D : stocker les mots de passe sous forme chiffrée

A.03.05.07.E : sélectionner un nouveau mot de passe lors de la première utilisation à la suite d'une récupération de compte

A.03.05.07.F : appliquer aux mots de passe les règles de composition et de complexité suivantes : **<A.03.05.07.ODP[02] : règles>**

Méthodes et objets d'évaluation potentiels :

Examen

[Sélection parmi les options suivantes : politique et procédures d'identification et d'authentification; stratégie de mot de passe; procédures liées à la gestion des authentifiants; documents sur la conception du système; paramètres de configuration du système; configurations des mots de passe; plan de sécurité du système; autres documents ou enregistrements pertinents]

Entrevue

[Sélection parmi les options suivantes : personnel responsable de la gestion des authentifiants; personnel responsable de la sécurité de l'information; développeuses et développeurs de système; administratrices et administrateurs de système]

Test

[Sélection parmi les options suivantes : mécanismes de prise en charge ou de mise en œuvre d'une capacité de gestion des authentifiants basée sur mot de passe]

Références :

Procédure d'évaluation tirée de la source : IA-05(01)

03.05.08 Non affecté

Retiré par le NIST.

03.05.09 Non affecté

Retiré par le NIST.

03.05.10 Non affecté

Retiré par le NIST.

03.05.11 Réinjection d'authentification

Confirmer l'exécution des actions suivantes :

A.03.05.11 : obscurcir les réinjections d'information durant le processus d'authentification

Méthodes et objets d'évaluation potentiels :

Examen

[Sélection parmi les options suivantes : politique et procédures d'identification et d'authentification; procédures liées à la réinjection d'authentification; documents sur la conception du système; paramètres de configuration du système; enregistrements de vérification du système; plan de sécurité du système; autres documents ou enregistrements pertinents]

Entrevue

[Sélection parmi les options suivantes : personnel responsable de la sécurité de l'information; développeuses et développeurs de système; administratrices et administrateurs de système]

Test

[Sélection parmi les options suivantes : mécanismes de prise en charge ou de mise en œuvre de l'obscurcissement des réinjections d'information durant le processus d'authentification]

Références :

Procédure d'évaluation tirée de la source : IA-06

03.05.12 Gestion des authentifiants

ODP :

A.03.05.12.ODP[01] : définir la fréquence à laquelle il convient de changer ou d'actualiser les authentifiants

A.03.05.12.ODP[02] : définir les événements qui déclenchent le changement ou l'actualisation des authentifiants

Confirmer l'exécution des actions suivantes :

A.03.05.12.A : vérifier, au moment de la distribution initiale d'un authentifiant, l'identité de l'utilisatrice ou utilisateur, du groupe, du rôle, du service ou du dispositif recevant l'authentifiant

A.03.05.12.B : établir le contenu de l'authentifiant initial pour les authentifiants émis par l'organisation

A.03.05.12.C[01] : établir des procédures administratives pour la distribution initiale des authentifiants

A.03.05.12.C[02] : établir des procédures administratives en cas de perte, de compromission ou de corruption des authentifiants

A.03.05.12.C[03] : établir des procédures administratives en cas de révocation des authentifiants

A.03.05.12.C[04] : mettre en œuvre des procédures administratives pour la distribution initiale des authentifiants

A.03.05.12.C[05] : mettre en œuvre des procédures administratives en cas de perte, de compromission ou de corruption des authentifiants

A.03.05.12.C[06] : mettre en place des procédures administratives en cas de révocation des authentifiants

A.03.05.12.D : changer les authentifiants par défaut lors de la première utilisation

A.03.05.12.E : changer ou actualiser les authentifiants tous les **<A.03.05.12.ODP[01] : fréquence>** ou lorsque les événements suivants se produisent : **<A.03.05.12.ODP[02] : événements>**

A.03.05.12.F[01] : protéger le contenu des authentifiants contre les divulgations non autorisées

A.03.05.12.F[02] : protéger le contenu des authentifiants contre les modifications non autorisées

Méthodes et objets d'évaluation potentiels :

Examen

[Sélection parmi les options suivantes : politique et procédures d'identification et d'authentification; procédures liées à la gestion des authentifiants; paramètres de configuration du système; liste des types d'authentifiants du système; documents sur la conception du système; enregistrements de vérification du système; enregistrements de contrôle des changements associés à la gestion des authentifiants du système; plan de sécurité du système; autres documents ou enregistrements pertinents]

Entrevue

[Sélection parmi les options suivantes : personnel responsable de la gestion des authentifiants; personnel responsable de la sécurité de l'information; administratrices et administrateurs de système]

Test

[Sélection parmi les options suivantes : mécanismes de prise en charge ou de mise en œuvre de la capacité de gestion des authentifiants]

Références :

Procédure d'évaluation tirée de la source : IA-05

3.6 Intervention en cas d'incident

Les contrôles de la famille Intervention en cas d'incident appuient l'établissement de capacités de traitement d'incident opérationnel pour les systèmes organisationnels, y compris :

- la préparation adéquate;
- la surveillance;
- la détection;
- l'analyse;
- le confinement;
- la reprise;

- l'intervention.

Les incidents sont surveillés, documentés et signalés aux autorités et aux responsables organisationnels appropriés.

03.06.01 Traitement des incidents

Confirmer l'exécution des actions suivantes :

A.03.06.01[01] : mettre en œuvre des capacités de traitement pour les incidents qui sont alignées sur le plan d'interventions en cas d'incident

A.03.06.01[02] : inclure les activités de préparation dans les capacités de traitement pour les incidents

A.03.06.01[03] : inclure les activités de détection et d'analyse dans les capacités de traitement pour les incidents

A.03.06.01[04] : inclure les activités de confinement dans les capacités de traitement pour les incidents

A.03.06.01[05] : inclure les activités d'éradication dans les capacités de traitement pour les incidents

A.03.06.01[06] : inclure les activités de reprise dans les capacités de traitement pour les incidents

Méthodes et objets d'évaluation potentiels :

Examen

[Sélection parmi les options suivantes : politique et procédure d'intervention en cas d'incident; politique et procédures de planification d'urgence; procédures liées au traitement des incidents; procédures liées à la planification des interventions en cas d'incident; plan d'intervention en cas d'incident; planification d'urgence; enregistrements des examens et des approbations du plan d'intervention en cas d'incident; plan de sécurité du système; plan de protection de la vie privée; autres documents ou enregistrements pertinents]

Entrevue

[Sélection parmi les options suivantes : personnel responsable du traitement des incidents; personnel responsable de la planification des interventions en cas d'incident; personnel responsable de la planification d'urgence; personnel responsable de la sécurité de l'information et de la protection de la vie privée]

Test

[Sélection parmi les options suivantes : capacités de traitement des incidents pour l'organisation; plan d'intervention en cas d'incident]

Références :

Procédure d'évaluation tirée de la source : IR-04

03.06.02 Surveillance des incidents, signalement des incidents et assistance en cas d'incident

ODP :

A.03.06.02.ODP[01] : définir le délai après lequel les incidents suspects doivent être signalés à l'équipe d'intervention en cas d'incident de l'organisation

A.03.06.02.ODP[02] : définir les autorités à qui l'information liée à un incident doit être signalée

Confirmer l'exécution des actions suivantes :

A.03.06.02.A[01] : faire le suivi des incidents de sécurité du système

A.03.06.02.A[02] : documenter les incidents de sécurité du système

A.03.06.02.B : exiger que les incidents suspects soient signalés à l'équipe d'intervention en cas d'incident de l'organisation dans <**A.03.06.02.ODP[01]** : délai>

A.03.06.02.C : transmettre l'information liée à un incident à <**A.03.06.02.ODP[02]** : autorités>

A.03.06.02.D : fournir une ressource de soutien pour l'intervention en cas d'incident qui offre des conseils et de l'assistance aux utilisatrices et utilisateurs du système pour ce qui touche le traitement et le signalement des incidents

Méthodes et objets d'évaluation potentiels :

Examen

[Sélection parmi les options suivantes : politique et procédure d'intervention en cas d'incident; procédures liées à la surveillance des incidents; procédures liées à l'assistance en cas d'incident; enregistrements et documents sur l'intervention en cas d'incident; plan d'intervention en cas d'incident; plan de sécurité du système; plan de protection de la vie privée; autres documents ou enregistrements pertinents]

Entrevue

[Sélection parmi les options suivantes : personnel responsable du traitement des incidents; personnel responsable de l'assistance et du soutien lors d'interventions en cas d'incident; personnel responsable de la sécurité de l'information et de la protection de la vie privée]

Test

[Sélection parmi les options suivantes : processus liés au signalement des incidents; capacité de surveillance des incidents; mécanismes de prise en charge ou de mise en œuvre du suivi et de la documentation des incidents de sécurité du système; mécanismes de prise en charge ou de mise en œuvre du signalement des incidents; mécanismes de prise en charge ou de mise en œuvre de l'assistance en cas d'incident; processus liés à l'assistance en cas d'incident]

Références :

Procédures d'évaluation tirées de la source : IR-05, IR-06 et IR-07

03.06.03 Tests d'intervention en cas d'incident

ODP :

A.03.06.03.ODP : définir la fréquence à laquelle il convient de tester l'efficacité de la capacité d'intervention en cas d'incident pour le système

Confirmer l'exécution des actions suivantes :

A.03.06.03 : tester l'efficacité de la capacité d'intervention en cas d'incident tous les **<A.03.06.03.ODP : fréquence>**

Méthodes et objets d'évaluation potentiels :

Examen

[Sélection parmi les options suivantes : politique et procédure d'intervention en cas d'incident; politique et procédures de planification d'urgence; procédures liées aux tests relatifs aux interventions en cas d'incident; procédures liées aux tests relatifs à la planification d'urgence; matériel de tests relatifs aux interventions en cas d'incident; résultats des tests relatifs aux interventions en cas d'incident; plan des tests relatifs aux interventions en cas d'incident; plan d'intervention en cas d'incident; plan d'urgence; plan de sécurité du système; plan de protection de la vie privée; autres documents ou enregistrements pertinents]

Entrevue

[Sélection parmi les options suivantes : personnel responsable des tests relatifs aux interventions en cas d'incident; personnel responsable de la sécurité de l'information et de la protection de la vie privée]

Références :

Procédure d'évaluation tirée de la source : IR-03

03.06.04 Formation sur les interventions en cas d'incident

ODP :

A.03.06.04.ODP[01] : définir le délai dans lequel la formation sur les interventions en cas d'incident doit être fournie aux utilisatrices et utilisateurs du système

A.03.06.04.ODP[02] : définir la fréquence à laquelle il convient de fournir une formation sur l'intervention en cas d'incident aux utilisatrices et utilisateurs du système après la formation initiale

A.03.06.04.ODP[03] : définir la fréquence à laquelle il convient de passer en revue et de mettre à jour le contenu de la formation sur les interventions en cas d'incident

A.03.06.04.ODP[04] : définir les événements qui déclenchent l'examen du contenu de la formation sur les interventions en cas d'incident

Confirmer l'exécution des actions suivantes :

A.03.06.04.A.01 : fournir une formation sur les interventions en cas d'incident aux utilisatrices et utilisateurs du système en fonction des rôles et des responsabilités attribués dans les **<A.03.06.04.ODP[01] : délai>** après avoir été affectés à un rôle ou à des responsabilités d'intervention en cas d'incident ou après avoir obtenu l'accès au système

A.03.06.04.A.02 : fournir une formation sur les interventions en cas d'incident aux utilisatrices et utilisateurs du système en fonction des rôles et des responsabilités attribués lorsque des changements apportés au système l'exigent

A.03.06.04.A.03 : fournir une formation sur les interventions en cas d'incident aux utilisatrices et utilisateurs du système en fonction des rôles et des responsabilités attribués tous les **<A.03.06.04.ODP[02] : fréquence>** par la suite

A.03.06.04.B[01] : passer en revue le contenu de la formation sur les interventions en cas d'incident tous les **<A.03.06.04.ODP[03] : fréquence>**

A.03.06.04.B[02] : mettre à jour le contenu de la formation sur les interventions en cas d'incident tous les **<A.03.06.04.ODP[03] : fréquence>**

A.03.06.04.B[03] : passer en revue le contenu de la formation sur les interventions en cas d'incident à la suite de **<A.03.06.04.ODP[04] : événements>**

A.03.06.04.B[04] : mettre à jour le contenu de la formation sur les interventions en cas d'incident à la suite de **<A.03.06.04.ODP[04] : événements>**

Méthodes et objets d'évaluation potentiels :

Examen

[Sélection parmi les options suivantes : politique et procédure d'intervention en cas d'incident; procédures liées à la formation sur les interventions en cas d'incident; programme de la formation sur les interventions en cas d'incident; matériel de la formation sur les interventions en cas d'incident; plan d'intervention en cas d'incident; enregistrements de la formation sur les interventions en cas d'incident; plan de sécurité du système; plan de protection de la vie privée; autres documents ou enregistrements pertinents]

Entrevue

[Sélection parmi les options suivantes : personnel responsable des activités et de la formation sur les interventions en cas d'incident; personnel responsable de la sécurité de l'information et de la protection de la vie privée]

Références :

Procédure d'évaluation tirée de la source : IR-02

03.06.05 Plan d'intervention en cas d'incident

Confirmer l'exécution des actions suivantes :

A.03.06.05.A.01 : élaborer un plan d'intervention en cas d'incident qui fournit à l'organisation une feuille de route pour la mise en œuvre de ses capacités d'intervention en cas d'incident

A.03.06.05.A.02 : élaborer un plan d'intervention en cas d'incident qui décrit la structure et l'organisation des capacités d'intervention en cas d'incident

A.03.06.05.A.03 : élaborer un plan d'intervention en cas d'incident qui fournit une approche de haut niveau indiquant comment les capacités d'intervention en cas d'incident s'intègrent à l'organisation en général

A.03.06.05.A.04 : élaborer un plan d'intervention en cas d'incident qui définit les incidents devant être signalés

A.03.06.05.A.05 : élaborer un plan d'intervention en cas d'incident qui décrit les modalités d'échange d'information en cas d'incident

A.03.06.05.A.06 : élaborer un plan d'intervention en cas d'incident qui désigne les responsabilités pour les entités, le personnel et les rôles organisationnels

A.03.06.05.B[01] : distribuer les copies du plan d'intervention en cas d'incident au personnel responsable de l'intervention en cas d'incident désigné (identifié par nom ou rôle)

A.03.06.05.B[02] : distribuer les copies du plan d'intervention en cas d'incident aux éléments organisationnels

A.03.06.05.C : mettre à jour le plan d'intervention en cas d'incident afin de tenir compte des changements apportés aux systèmes et des changements organisationnels, ou encore des problèmes rencontrés durant la mise en œuvre, l'exécution ou la mise à l'essai du plan d'intervention

A.03.06.05.D : protéger le plan d'intervention en cas d'incident contre les divulgations non autorisées

Méthodes et objets d'évaluation potentiels :

Examen

[Sélection parmi les options suivantes : politique d'intervention en cas d'incident; procédures liées au plan d'intervention en cas d'incident; plan d'intervention en cas d'incident; plan de sécurité du système; plan de protection de la vie privée; enregistrements des examens et des approbations du plan d'intervention en cas d'incident; autres documents ou enregistrements pertinents]

Entrevue

[Sélection parmi les options suivantes : personnel responsable de la planification des interventions en cas d'incident; personnel responsable de la sécurité de l'information et de la protection de la vie privée]

Test

[Sélection parmi les options suivantes : plan d'intervention en cas d'incident et processus connexes]

Références :

Procédure d'évaluation tirée de la source : IR-08

3.7 Maintenance

Les contrôles de la famille Maintenance appuient la maintenance périodique et opportune des systèmes organisationnels et fournissent des contrôles efficaces pour les outils, les techniques, les mécanismes et le personnel employés pour mener la maintenance des systèmes afin d'assurer leur disponibilité continue.

03.07.01 Non affecté

Retiré par le NIST.

03.07.02 Non affecté

Retiré par le NIST.

03.07.03 Non affecté

Retiré par le NIST.

03.07.04 Outils de maintenance

Confirmer l'exécution des actions suivantes :

A.03.07.04.A[01] : approuver l'utilisation des outils de maintenance du système

A.03.07.04.A[02] : contrôler l'utilisation des outils de maintenance du système

A.03.07.04.A[03] : surveiller l'utilisation des outils de maintenance du système

A.03.07.04.B : vérifier les supports où sont exécutés les programmes de diagnostic et de test afin de détecter la présence de code malveillant avant d'utiliser les supports dans le système

A.03.07.04.C : prévenir le retrait d'équipement de maintenance de système qui pourrait contenir de l'information désignée et vérifier qu'il ne contient pas une telle information, en procédant à des opérations de nettoyage ou de destruction de l'équipement ou encore en conservant l'équipement dans l'installation

Méthodes et objets d'évaluation potentiels :

Examen

[Sélection parmi les options suivantes : politique et procédures de maintenance; procédures liées aux outils de maintenance du système; outils de maintenance du système; enregistrements d'inspection des outils de maintenance; enregistrements de nettoyage de l'équipement; enregistrements de nettoyage des supports; plan de sécurité du système; autres documents ou enregistrements pertinents]

Entrevue

[Sélection parmi les options suivantes : personnel responsable de la maintenance du système; personnel responsable du nettoyage des supports; personnel responsable de la sécurité de l'information]

Test

[Sélection parmi les options suivantes : processus liés à l'approbation, au contrôle et à la surveillance des outils de maintenance; mécanismes de prise en charge ou de mise en œuvre de l'approbation, du contrôle ou de la surveillance des outils de maintenance; processus liés à la prévention du retrait non autorisé de l'information; processus liés à l'inspection du code malveillant; mécanismes liés à la prise en charge du nettoyage des supports ou de la destruction de l'équipement; mécanismes liés à la prise en charge de la vérification du nettoyage des supports; processus liés à l'inspection des outils de maintenance; mécanismes de prise en charge ou de mise en œuvre de l'inspection des outils de maintenance; mécanismes de prise en charge ou de mise en œuvre de l'inspection des supports utilisés aux fins de maintenance]

Références :

Procédures d'évaluation tirées de la source : MA-03, MA-03(01), MA-03(02) et MA-03(03)

03.07.05 Maintenance non locale**Confirmer l'exécution des actions suivantes :**

A.03.07.05.A[01] : approuver les activités de maintenance et de diagnostic non locales

A.03.07.05.A[02] : surveiller les activités de maintenance et de diagnostic non locales

A.03.07.05.B[01] : mettre en œuvre des mécanismes d'AMF lors de l'établissement des sessions de maintenance et de diagnostic non locales

A.03.07.05.B[02] : mettre en œuvre une résistance à la réinsertion lors de l'établissement des sessions de maintenance et de diagnostic non locales

A.03.07.05.C[01] : mettre fin aux sessions lorsque la maintenance non locale est terminée

A.03.07.05.C[02] : mettre fin aux connexions réseau lorsque la maintenance non locale est terminée

Méthodes et objets d'évaluation potentiels :**Examen**

[Sélection parmi les options suivantes : politique et procédures de maintenance; politique et procédures d'accès à distance; procédures liées à la maintenance de systèmes non locaux; enregistrements d'accès à distance; enregistrements de maintenance; enregistrements de diagnostic; documents sur la conception du système; paramètres de configuration du système; plan de sécurité du système; autres documents ou enregistrements pertinents]

Entrevue

[Sélection parmi les options suivantes : personnel responsable de la maintenance du système; personnel responsable de la sécurité de l'information; administratrices et administrateurs de système]

Test

[Sélection parmi les options suivantes : processus liés à la gestion de la maintenance non locale; mécanismes liés à la mise en œuvre, à la prise en charge ou à la gestion de la maintenance non locale; mécanismes liés à la mise en œuvre de l'AMF et à la résistance à la réinsertion; mécanismes liés à l'interruption des sessions de maintenance et des connexions réseau non locales]

Références :

Procédure d'évaluation tirée de la source : MA-04

03.07.06 Personnel de maintenance**Confirmer l'exécution des actions suivantes :**

A.03.07.06.A : établir un processus d'autorisation du personnel de maintenance

A.03.07.06.B : tenir à jour une liste des organisations ou du personnel autorisé à effectuer les activités de maintenance

A.03.07.06.C : vérifier que le personnel non accompagné réalisant des activités de maintenance sur le système dispose des autorisations d'accès nécessaires

A.03.07.06.D[01] : désigner des membres du personnel de l'organisation qui possèdent les autorisations d'accès nécessaires pour superviser les activités de maintenance effectuées par le personnel qui ne possède pas les autorisations d'accès appropriées

A.03.07.06.D[02] : désigner des membres du personnel de l'organisation qui possèdent les compétences techniques nécessaires pour superviser les activités de maintenance effectuées par le personnel qui ne possède pas les autorisations d'accès appropriées

Méthodes et objets d'évaluation potentiels :

Examen

[Sélection parmi les options suivantes : politique et procédures de maintenance; contrats des fournisseurs de services; accords sur les niveaux de service; liste du personnel autorisé; enregistrements de maintenance; enregistrements de contrôle d'accès; plan de sécurité du système; autres documents ou enregistrements pertinents]

Entrevue

[Sélection parmi les options suivantes : personnel responsable de la maintenance du système; personnel responsable de la sécurité de l'information]

Test

[Sélection parmi les options suivantes : processus liés à l'autorisation et à la gestion du personnel de maintenance; mécanismes de prise en charge ou de mise en œuvre de l'autorisation du personnel de maintenance]

Références :

Procédure d'évaluation tirée de la source : MA-05

3.8 Protection des supports

Les contrôles de la famille Protection des supports appuient la protection des supports du système tout au long du cycle de vie. Ils permettent de limiter l'accès à l'information sur les supports du système aux utilisatrices et utilisateurs autorisés et exigent un nettoyage ou une destruction des supports avant leur élimination ou leur réutilisation.

03.08.01 Entreposage des supports

Confirmer l'exécution des actions suivantes :

A.03.08.01[01] : contrôler physiquement les supports du système qui contiennent de l'information désignée

A.03.08.01[02] : entreposer de façon sécurisée les supports du système qui contiennent de l'information désignée

Méthodes et objets d'évaluation potentiels :**Examen**

[Sélection parmi les options suivantes : politique et procédures de protection physique; politique et procédures de protection des supports; procédures liées à l'entreposage des supports; politique et procédures de contrôle d'accès; supports du système; plan de sécurité du système; autres documents ou enregistrements pertinents]

Entrevue

[Sélection parmi les options suivantes : personnel responsable de la protection et de l'entreposage des supports du système; personnel responsable de la sécurité de l'information]

Test

[Sélection parmi les options suivantes : processus liés à l'entreposage des supports contenant de l'information; mécanismes de prise en charge ou de mise en œuvre de la protection des supports ou de l'entreposage des supports de façon sécurisée]

Références :

Procédure d'évaluation tirée de la source : MP-04

03.08.02 Accès aux supports**Confirmer l'exécution des actions suivantes :**

A.03.08.02 : restreindre l'accès à l'information désignée qui se trouve sur les supports du système au personnel ou aux rôles autorisés

Méthodes et objets d'évaluation potentiels :**Examen**

[Sélection parmi les options suivantes : politique et procédures de protection physique; politique et procédures de protection des supports; procédures liées à la restriction de l'accès aux supports; politique et procédures de contrôle d'accès; installations d'entreposage des supports; enregistrements de contrôle d'accès; plan de sécurité du système; autres documents ou enregistrements pertinents]

Entrevue

[Sélection parmi les options suivantes : personnel responsable de la protection des supports du système; personnel responsable de la sécurité de l'information; administratrices et administrateurs de système]

Test

[Sélection parmi les options suivantes : processus liés à la restriction de l'information sur les supports; mécanismes de prise en charge ou de mise en œuvre des restrictions d'accès aux supports]

Références :

Procédure d'évaluation tirée de la source : MP-02

03.08.03 Nettoyage des supports

Confirmer l'exécution des actions suivantes :

A.03.08.03 : nettoyer les supports du système qui contiennent de l'information désignée avant leur élimination ou leur transfert hors du contrôle de l'organisation ou aux fins de réutilisation

Méthodes et objets d'évaluation potentiels :

Examen

[Sélection parmi les options suivantes : politique et procédures de protection des supports; procédures de nettoyage et d'élimination des supports; normes et stratégies applicables qui traitent de la politique de nettoyage des supports; enregistrements de vérification du système; enregistrements de nettoyage de supports; documents sur la conception du système; paramètres de configuration du système; politique sur la conservation et la disposition des documents; procédures de conservation et de disposition des documents; plan de sécurité du système; plan de protection de la vie privée; autres documents et enregistrements pertinents]

Entrevue

[Sélection parmi les options suivantes : personnel responsable du nettoyage des supports; personnel responsable de la conservation et de la disposition des documents; personnel responsable de la sécurité de l'information et de la protection de la vie privée; administratrices et administrateurs de système]

Test

[Sélection parmi les options suivantes : processus de nettoyage des supports; mécanismes pour la prise en charge et la mise en œuvre du nettoyage des supports]

Références :

Procédure d'évaluation tirée de la source : MP-06

03.08.04 Marquage des supports

Confirmer l'exécution des actions suivantes :

A.03.08.04[01] : marquer les supports contenant de l'information désignée afin d'indiquer les limites de distribution

A.03.08.04[02] : marquer les supports contenant de l'information désignée afin d'indiquer les mises en garde concernant le traitement

A.03.08.04[03] : marquer les supports contenant de l'information désignée afin d'indiquer les marquages applicables d'une telle information

Méthodes et objets d'évaluation potentiels :

Examen

[Sélection parmi les options suivantes : politique et procédures de protection physique; politique et procédures de protection des supports; procédures liées au marquage des supports; liste des attributs de sécurité du marquage des supports; plan de sécurité du système; autres documents ou enregistrements pertinents]

Entrevue

[Sélection parmi les options suivantes : personnel responsable de la protection et du marquage des supports du système; personnel responsable de la sécurité de l'information]

Test

[Sélection parmi les options suivantes : processus liés au marquage des supports contenant de l'information; mécanismes de prise en charge ou de mise en œuvre du marquage des supports]

Références :

Procédure d'évaluation tirée de la source : MP-03

03.08.05 Transport des supports**Confirmer l'exécution des actions suivantes :**

A.03.08.05.A[01] : protéger les supports du système contenant de l'information désignée durant le transport à l'extérieur des zones contrôlées

A.03.08.05.A[02] : contrôler les supports du système contenant de l'information désignée durant le transport à l'extérieur des zones contrôlées

A.03.08.05.B: demeurer responsable des supports du système contenant de l'information désignée durant le transport à l'extérieur des zones contrôlées

A.03.08.05.C : documenter les activités associées au transport des supports du système contenant de l'information désignée

Méthodes et objets d'évaluation potentiels :**Examen**

[Sélection parmi les options suivantes : politique et procédures de protection physique; politique et procédures de protection des supports; procédures liées à l'entreposage des supports; politique et procédures de contrôle d'accès; liste du personnel autorisé; supports du système; zones contrôlées désignées; politique et procédures de protection des systèmes et des communications; documents sur les mécanismes cryptographiques et la conception; procédures liées à la protection de l'information au repos; documents sur la conception du système; paramètres de configuration du système; liste de l'information au repos dont la confidentialité doit être protégée; enregistrements de vérification du système; plan de sécurité du système; autres documents ou enregistrements pertinents]

Entrevue

[Sélection parmi les options suivantes : personnel responsable de la protection et de l'entreposage des supports du système; personnel responsable de la sécurité de l'information; développeuses et développeurs de système; administratrices et administrateurs de système]

Test

[Sélection parmi les options suivantes : processus liés à l'entreposage des supports contenant de l'information; mécanismes de prise en charge ou de mise en œuvre de l'entreposage ou de la protection des supports; mécanismes de prise en charge ou de mise en œuvre des mesures de protection de la confidentialité pour l'information au repos]

Références :

Procédures d'évaluation tirées de la source : MP-05 et SC-28

03.08.06 Non affecté

Retiré par le NIST.

03.08.07 Utilisation des supports**ODP :**

A.03.08.07.ODP : définir les types de supports dont l'utilisation est interdite ou soumise à des restrictions

Confirmer l'exécution des actions suivantes :

A.03.08.07.A : restreindre ou interdire l'utilisation des types de supports suivants : **<A.03.08.07.ODP : types de supports du système>**

A.03.08.07.B : interdire l'utilisation de supports amovibles sans la présence d'une ou un propriétaire identifiable

Méthodes et objets d'évaluation potentiels :**Examen**

[Sélection parmi les options suivantes : politique et procédures de protection des supports du système; politique sur l'utilisation du système; procédures liées aux restrictions relatives à l'utilisation des supports; règles de conduite; enregistrements de vérification du système; documents sur la conception du système; paramètres de configuration du système; plan de sécurité du système; autres documents ou enregistrements pertinents]

Entrevue

[Sélection parmi les options suivantes : personnel responsable de l'utilisation des supports du système; personnel responsable de la sécurité de l'information; administratrices et administrateurs de système]

Test

[Sélection parmi les options suivantes : processus liés à l'utilisation des supports; mécanismes liés à la restriction ou à l'interdiction de l'utilisation des supports sur le système ou les composants du système]

Références :

Procédure d'évaluation tirée de la source : MP-07

03.08.08 Non affecté

Retiré par le NIST.

03.08.09 Sauvegarde du système – Protection cryptographique

Confirmer l'exécution des actions suivantes :

A.03.08.09.A : protéger la confidentialité de l'information sauvegardée

A.03.08.09.B : mettre en œuvre des mécanismes cryptographiques afin d'empêcher la divulgation non autorisée d'information désignée aux emplacements de stockage des sauvegardes

Méthodes et objets d'évaluation potentiels :

Examen

[Sélection parmi les options suivantes : politique et procédures de planification d'urgence; procédures liées à la sauvegarde du système; plan d'urgence; documents sur la conception du système; paramètres de configuration du système; plan de sécurité du système; autres documents ou enregistrements pertinents]

Entrevue

[Sélection parmi les options suivantes : personnel responsable de la sauvegarde du système; personnel responsable de la sécurité de l'information]

Test

[Sélection parmi les options suivantes : mécanismes de prise en charge ou de mise en œuvre de la protection cryptographique de l'information de sauvegarde]

Références :

Procédures d'évaluation tirées de la source : CP-09 et CP-09(08)

3.9 Sécurité du personnel

Les contrôles de la famille Sécurité du personnel appuient les procédures requises pour s'assurer que le personnel ayant accès aux systèmes dispose des autorisations nécessaires et des niveaux d'habilitation de sécurité appropriés. Ils contribuent à protéger l'information organisationnelle et les systèmes durant et après les actions du personnel, par exemple après une cessation d'emploi ou une mutation.

03.09.01 Filtrage de sécurité du personnel

ODP :

A.03.09.01.ODP : définir les conditions qui exigent un nouveau filtrage de sécurité des personnes

Confirmer l'exécution des actions suivantes :

A.03.09.01.A : procéder au filtrage de sécurité des personnes avant de leur accorder l'accès au système

A.03.09.01.B : effectuer un nouveau filtrage de sécurité lorsque les conditions suivantes l'exigent : **<A.03.09.01.ODP : conditions>**

Méthodes et objets d'évaluation potentiels :**Examen**

[Sélection parmi les options suivantes : politique et procédures de sécurité du personnel; procédures liées au filtrage de sécurité ou à un nouveau filtrage de sécurité du personnel; enregistrements du personnel ayant fait l'objet d'un filtrage de sécurité; plan de sécurité du système; autres documents ou enregistrements pertinents]

Entrevue

[Sélection parmi les options suivantes : personnel responsable de la sécurité du personnel; personnel responsable de la sécurité de l'information]

Test

[Sélection parmi les options suivantes : processus liés au filtrage de sécurité ou à un nouveau filtrage de sécurité du personnel]

Références :

Procédure d'évaluation tirée de la source : PS-03

03.09.02 Cessation d'emploi et mutation de personnel**ODP :**

A.03.09.02.ODP: définir les délais dans lesquels il convient de désactiver l'accès au système

Confirmer l'exécution des actions suivantes :

A.03.09.02.A.01 : lors de la cessation d'emploi d'une employée ou un employé, mettre un terme à l'accès au système dans les **<A.03.09.02.ODP : délai>**

A.03.09.02.A.02[01] : lors de la cessation d'emploi d'une employée ou un employé, mettre fin ou révoquer les authentifiants associés à cette personne

A.03.09.02.A.02[02] : lors de la cessation d'emploi d'une employée ou un employé, mettre fin ou révoquer les justificatifs d'identité associés à cette personne

A.03.09.02.A.03 : lors de la cessation d'emploi d'une employée ou un employé, récupérer les propriétés système associées à la sécurité

A.03.09.02.B.01[01] : examiner les exigences opérationnelles liées aux autorisations d'accès physiques et logiques existantes aux systèmes et aux installations lorsque des employées et employés sont réaffectés ou transférés à d'autres postes au sein de l'organisation

A.03.09.02.B.01[02] : confirmer les exigences opérationnelles liées aux autorisations d'accès physiques et logiques existantes aux systèmes et aux installations lorsque des employés et employées sont réaffectés ou transférés à d'autres postes au sein de l'organisation

A.03.09.02.B.02 : modifier l'autorisation d'accès liée à tout changement dans les exigences opérationnelles lorsque des employés et employées sont réaffectés ou transférés à d'autres postes au sein de l'organisation

Méthodes et objets d'évaluation potentiels :

Examen

[Sélection parmi les options suivantes : politique et procédures de sécurité du personnel; procédures liées à la cessation d'emploi du personnel; enregistrements des mesures de transfert du personnel; procédures liées au transfert du personnel; liste des autorisations d'accès aux installations et aux systèmes; enregistrements sur les mesures de cessation d'emploi du personnel; enregistrements sur les authentifiants ou les justificatifs d'identité désactivés ou révoqués; liste des comptes du système; enregistrements des entrevues de fin d'emploi; plan de sécurité du système; autres documents ou enregistrements pertinents]

Entrevue

[Sélection parmi les options suivantes : personnel responsable de la sécurité du personnel; personnel responsable de la gestion des comptes; personnel responsable de la sécurité de l'information; administratrices et administrateurs de système]

Test

[Sélection parmi les options suivantes : processus liés à la cessation d'emploi du personnel; processus liés au transfert du personnel; mécanismes liés de prise en charge ou de mise en œuvre des notifications de transfert du personnel; mécanismes de prise en charge ou de mise en œuvre des notifications de cessation d'emploi du personnel; mécanismes liés à la désactivation de l'accès au système et à la révocation des authentifiants]

Références :

Procédures d'évaluation tirées de la source : PS-04 et PS-05

3.10 Protection matérielle

Les contrôles de la famille Protection matérielle appuient le contrôle de l'accès physique des personnes autorisées aux systèmes, à l'équipement et aux environnements d'exploitation respectifs. Ils favorisent la protection des installations physiques et des infrastructures des systèmes ainsi que la protection des systèmes contre les dangers environnementaux. Ils fournissent également des contrôles environnementaux appropriés pour les installations hébergeant des systèmes.

03.10.01 Autorisations d'accès physique

ODP :

A.03.10.01.ODP : définir la fréquence à laquelle il convient de passer en revue la liste d'accès qui fournit les détails quant aux personnes autorisées à y accéder physiquement

Confirmer l'exécution des actions suivantes :

A.03.10.01.A[01] : créer une liste des personnes disposant d'un accès autorisé à l'installation où se trouve le système

A.03.10.01.A[02] : approuver une liste des personnes disposant d'un accès autorisé à l'installation où se trouve le système

A.03.10.01.A[03] : tenir à jour une liste des personnes disposant d'un accès autorisé à l'installation où se trouve le système

A.03.10.01.B : émettre les justificatifs d'autorisation pour accéder à l'installation

A.03.10.01.C : passer en revue la liste des accès physiques tous les **<A.03.10.01.ODP : fréquence>**

A.03.10.01.D : retirer les personnes de la liste d'accès aux installations lorsqu'un tel accès n'est plus nécessaire

Méthodes et objets d'évaluation potentiels :**Examen**

[Sélection parmi les options suivantes : politique et procédures de protection physique; procédures d'autorisation de l'accès physique; liste d'accès du personnel autorisé; examens de la liste d'accès physique; enregistrements de résiliation de l'accès physique; justificatifs d'autorisation; plan de sécurité du système; autres documents ou enregistrements pertinents]

Entrevue

[Sélection parmi les options suivantes : personnel responsable des autorisations d'accès physique; personnel disposant d'un accès physique à l'installation où se trouve le système; personnel responsable de la sécurité de l'information]

Test

[Sélection parmi les options suivantes : processus pour les autorisations d'accès physique; mécanismes de prise en charge ou de mise en œuvre des autorisations d'accès physique]

Références :

Procédure d'évaluation tirée de la source : PE-02

03.10.02 Surveillance de l'accès physique**ODP :**

A.03.10.02.ODP[01] : définir la fréquence à laquelle il convient de passer en revue les journaux d'accès physique

A.03.10.02.ODP[02] : définir les événements ou les indications potentielles d'événement pour lesquels il convient d'examiner les journaux d'accès physique

Confirmer l'exécution des actions suivantes :

A.03.10.02.A[01] : surveiller l'accès physique aux installations où se trouvent les systèmes afin de détecter les incidents de sécurité physique

A.03.10.02.A[02] : intervenir en cas d'incident de sécurité physique

A.03.10.02.B[01] : examiner les journaux d'accès physique tous les **<A.03.10.02.ODP[01] : fréquence>**

A.03.10.02.B[02] : examiner les journaux d'accès physique à la suite de <**A.03.10.02.ODP[02]** : événements ou indications potentielles d'événement>

Méthodes et objets d'évaluation potentiels :

Examen

[Sélection parmi les options suivantes : politique et procédures de protection physique; procédures liées à la surveillance de l'accès physique; journaux ou enregistrements de l'accès physique; enregistrements de surveillance de l'accès physique; examens des journaux de l'accès physique; plan de sécurité du système; autres documents ou enregistrements pertinents]

Entrevue

[Sélection parmi les options suivantes : personnel responsable de la surveillance de l'accès physique; personnel responsable de l'intervention en cas d'incident; personnel responsable de la sécurité de l'information]

Test

[Sélection parmi les options suivantes : processus liés à la surveillance de l'accès physique; mécanismes de prise en charge ou de mise en œuvre de la surveillance de l'accès physique; mécanismes de prise en charge ou de mise en œuvre de l'examen des journaux de l'accès physique]

Références :

Procédure d'évaluation tirée de la source : PE-06

03.10.03 Non affecté

Retiré par le NIST.

03.10.04 Non affecté

Retiré par le NIST.

03.10.05 Non affecté

Retiré par le NIST.

03.10.06 Autres lieux de travail

ODP :

A.03.10.06.ODP : définir les exigences de sécurité à employer dans les autres lieux de travail

Confirmer l'exécution des actions suivantes :

A.03.10.06.A : déterminer les autres lieux de travail où le personnel peut travailler

A.03.10.06.B : employer les exigences de sécurité suivantes pour les autres lieux de travail : <**A.03.10.06.ODP** : exigences de sécurité>

Méthodes et objets d'évaluation potentiels :**Examen**

[Sélection parmi les options suivantes : politique et procédures de protection physique; procédures liées aux autres lieux de travail du personnel; liste des exigences de sécurité dans les autres lieux de travail; évaluations des exigences de sécurité dans les autres lieux de travail; plan de sécurité du système; plan de protection de la vie privée; autres documents ou enregistrements pertinents]

Entrevue

[Sélection parmi les options suivantes : personnel approuvant l'utilisation des autres lieux de travail; personnel utilisant d'autres lieux de travail; personnel évaluant les exigences de sécurité des autres lieux de travail; personnel responsable de la sécurité de l'information et de la protection de la vie privée]

Test

[Sélection parmi les options suivantes : processus liés à la sécurité et à la protection de la vie privée dans les autres lieux de travail; mécanismes liés au soutien des autres lieux de travail; exigences de sécurité et de protection de la vie privée employées dans les autres lieux de travail; moyens de communication entre le personnel dans les autres lieux de travail et le personnel de sécurité]

Références :

Procédure d'évaluation tirée de la source : PE-17

03.10.07 Contrôle d'accès physique**Confirmer l'exécution des actions suivantes :**

A.03.10.07.A.01 : appliquer les autorisations d'accès physique aux points d'entrée et de sortie dans les installations où se trouvent les systèmes en vérifiant les autorisations d'accès physique des individus avant d'accorder l'accès

A.03.10.07.A.02 : appliquer les autorisations d'accès physique aux points d'entrée et de sortie dans les installations où se trouvent les systèmes en contrôlant les points d'entrée et de sortie au moyen de systèmes de contrôle d'accès physique, de dispositifs ou de mécanismes de protection

A.03.10.07.B : tenir à jour les journaux de vérification d'accès physique pour les points d'entrée et de sortie

A.03.10.07.C[01] : accompagner les visiteuses et visiteurs

A.03.10.07.C[02] : contrôler l'activité des visiteuses et visiteurs

A.03.10.07.D : sécuriser les clés, les combinaisons et les autres dispositifs d'accès physique

A.03.10.07.E : contrôler l'accès physique aux dispositifs de sortie avant d'empêcher les personnes non autorisées d'obtenir l'accès à l'information désignée

Méthodes et objets d'évaluation potentiels :**Examen**

[Sélection parmi les options suivantes : politique et procédures de protection physique; procédures pour le contrôle d'accès physique; journaux ou registres de contrôle d'accès physique; registre d'inventaire des dispositifs de contrôle d'accès physique; points d'entrée et de sortie du système; enregistrements des changements de combinaisons et des clés; emplacements de stockage des dispositifs de contrôle d'accès physique; dispositifs de contrôle d'accès physique; liste des mécanismes de sécurité contrôlant l'accès aux zones désignées comme étant accessibles au public au sein de l'installation; plan de sécurité du système; autres documents et enregistrements pertinents]

Entrevue

[Sélection parmi les options suivantes : personnel responsable du contrôle d'accès physique; personnel responsable de la sécurité de l'information]

Test

[Sélection parmi les options suivantes : processus liés au contrôle de l'accès physique; mécanismes de prise en charge et de mise en œuvre d'un contrôle d'accès physique; dispositifs de contrôle de l'accès physique]

Références :

Procédure d'évaluation tirée de la source : PE-03 et PE-05

03.10.08 Contrôle d'accès pour la transmission**Confirmer l'exécution des actions suivantes :**

A.03.10.08 : contrôler l'accès physique aux lignes de distribution et de transmission dans les installations de l'organisation

Méthodes et objets d'évaluation potentiels :**Examen**

[Sélection parmi les options suivantes : politique et procédures de protection physique; procédures liées au contrôle de l'accès aux supports de transmission; documents sur la conception du système; schémas de câblage et des communications de l'installation; liste des mesures de sécurité physique appliquées aux lignes de distribution et de transmission du système; procédures pour le contrôle de l'accès aux supports d'affichage; aménagement des composants du système dans l'installation; liste des dispositifs de sortie et des périphériques connexes qui exigent des contrôles d'accès physique; affichage réel des composants du système; journaux ou enregistrements des contrôles d'accès physique pour les zones comportant des dispositifs de sortie et des périphériques connexes; plan de sécurité du système; autres documents ou enregistrements pertinents]

Entrevue

[Sélection parmi les options suivantes : personnel responsable du contrôle d'accès physique; personnel responsable de la sécurité de l'information]

Test

[Sélection parmi les options suivantes : processus liés au contrôle de l'accès aux lignes de distribution et de transmission; mécanismes de prise en charge ou de mise en œuvre des lignes de distribution et de transmission; processus liés au contrôle de l'accès aux dispositifs de sortie; mécanismes de prise en charge ou de mise en œuvre du contrôle de l'accès aux dispositifs de sortie]

Références :

Procédure d'évaluation tirée de la source : PE-04

3.11 Évaluation des risques

Les contrôles de la famille Évaluation des risques appuient la conduite périodique d'évaluations des risques, y compris les EFVP, qui peuvent découler de l'exploitation des systèmes organisationnels ou du traitement, du stockage ou de la transmission de données et d'information.

03.11.01 Évaluation des risques

ODP :

A.03.11.01.ODP : définir la fréquence à laquelle il convient de mettre à jour l'évaluation des risques

Confirmer l'exécution des actions suivantes :

A.03.11.01.A : évaluer le risque (y compris les risques associés à la chaîne d'approvisionnement) de divulgation non autorisée résultant du traitement, du stockage ou de la transmission de l'information désignée

A.03.11.01.B : mettre à jour les évaluations des risques tous les **<A.03.11.01.ODP : fréquence>**

Méthodes et objets d'évaluation potentiels :**Examen**

[Sélection parmi les options suivantes : politique et procédures liées à l'évaluation des risques; politique et procédures de planification de la sécurité et de la protection de la vie privée; procédures liées aux évaluations des risques de l'organisation; évaluation des risques; résultats de l'évaluation des risques; examens des évaluations des risques; mises à jour des évaluations des risques; politique et procédures liées à la gestion des risques liés à la chaîne d'approvisionnement (GRCA); inventaire des systèmes essentiels, des composants du système et des services qui s'y rapportent; procédures liées aux évaluations des risques liés à la chaîne d'approvisionnement de l'organisation; politique d'approvisionnement; plan de GRCA; plan de sécurité du système; plan de protection de la vie privée; autres documents ou enregistrements pertinents]

Entrevue

[Sélection parmi les options suivantes : personnel responsable de l'évaluation des risques; personnel responsable de la GRCA; personnel responsable de la sécurité et de la protection de la vie privée]

Test

[Sélection parmi les options suivantes : processus liés aux évaluations des risques de l'organisation; mécanismes de prise en charge ou de mise en œuvre de la réalisation, de la documentation, de l'examen, de la diffusion et de la mise à jour des évaluations des risques; mécanismes liés à la prise en charge ou à la réalisation, à la documentation, à l'examen, à la diffusion et à la mise à jour des évaluations des risques]

Références :

Procédures d'évaluation tirées de la source : RA-03, RA-03(01) et SR-06

03.11.02 Surveillance et analyse des vulnérabilités**ODP :**

A.03.11.02.ODP[01] : définir la fréquence à laquelle il convient de surveiller les vulnérabilités dans le système

A.03.11.02.ODP[02] : définir la fréquence à laquelle il convient d'analyser les vulnérabilités dans le système

A.03.11.02.ODP[03] : définir les délais d'exécution dans lesquels il convient de corriger les vulnérabilités du système

A.03.11.02.ODP[04] : définir la fréquence à laquelle il convient de mettre à jour les vulnérabilités du système à analyser

Confirmer l'exécution des actions suivantes :

A.03.11.02.A[01] : surveiller les vulnérabilités dans le système tous les **<A.03.11.02.ODP[01] : fréquence>**

A.03.11.02.A[02] : analyser les vulnérabilités dans le système tous les **<A.03.11.02.ODP[02] : fréquence>**

A.03.11.02.A[03] : surveiller les vulnérabilités dans le système lorsque de nouvelles vulnérabilités susceptibles d'influer sur le système sont identifiées

A.03.11.02.A[04] : analyser les vulnérabilités sur le système lorsque de nouvelles vulnérabilités susceptibles d'influer sur le système sont identifiées

A.03.11.02.B : corriger les vulnérabilités du système dans les **<A.03.11.02.ODP[03] : délais d'exécution>**

A.03.11.02.C[01] : mettre à jour la liste des vulnérabilités du système à analyser tous les **<A.03.11.02.ODP[04] : fréquence>**

A.03.11.02.C[02] : mettre à jour la liste des vulnérabilités du système à analyser lorsque de nouvelles vulnérabilités sont identifiées et signalées

Méthodes et objets d'évaluation potentiels :**Examen**

[Sélection parmi les options suivantes : politique et procédures d'évaluation des risques; procédures liées à l'analyse des vulnérabilités; enregistrements de gestion des correctifs et des vulnérabilités; documents sur la configuration et les outils d'analyse des vulnérabilités; résultats de l'analyse des vulnérabilités; évaluation des risques; rapport d'évaluation des risques; plan de sécurité du système; autres documents ou enregistrements pertinents]

Entrevue

[Sélection parmi les options suivantes : personnel responsable de l'évaluation des risques et de l'analyse des vulnérabilités; personnel responsable de l'étude de l'analyse des vulnérabilités; personnel responsable de l'atténuation des vulnérabilités; personnel responsable de la sécurité de l'information; administratrices et administrateurs de système]

Test

[Sélection parmi les options suivantes : processus liés à la surveillance, à l'analyse, à l'étude et à l'atténuation des vulnérabilités; mécanismes de prise en charge ou de mise en œuvre de la surveillance, de l'analyse, de l'étude et de l'atténuation des vulnérabilités]

Références :

Procédures d'évaluation tirées de la source : RA-05 et RA-05(02)

03.11.03 Non affecté

Retiré par le NIST.

03.11.04 Réponse aux risques**Confirmer l'exécution des actions suivantes :**

A.03.11.04[01] : prendre des mesures à l'égard des résultats des évaluations de la sécurité

A.03.11.04[02] : prendre des mesures à l'égard des résultats de la surveillance de la sécurité

A.03.11.04[03] : prendre des mesures à l'égard des résultats des vérifications de la sécurité

Méthodes et objets d'évaluation potentiels :**Examen**

[Sélection parmi les options suivantes : politique d'évaluation des risques; rapports d'évaluation; enregistrements de vérification du système; journaux des événements; plan de sécurité du système; plan de protection de la vie privée; autres documents ou enregistrements pertinents]

Entrevue

[Sélection parmi les options suivantes : personnel responsable de l'évaluation et de la vérification; administratrices et administrateurs de système; personnel responsable de la sécurité et de la protection de la vie privée]

Test

[Sélection parmi les options suivantes : processus liés aux évaluations et aux vérifications; mécanismes et outils liés à la prise en charge ou à la mise en œuvre des évaluations et des vérifications]

Références :

Procédure d'évaluation tirée de la source : RA-07

3.12 Évaluation de sécurité et surveillance

Les contrôles de la famille Évaluation de sécurité et surveillance traitent des évaluations de sécurité et des mécanismes de surveillance du système.

03.12.01 Évaluation de sécurité

ODP :

A.03.12.01.ODP : définir la fréquence à laquelle il convient d'évaluer les exigences de sécurité du système et de l'environnement dans lequel il est exploité

Confirmer l'exécution des actions suivantes :

A.03.12.01 : évaluer les exigences de sécurité du système et de l'environnement dans lequel il est exploité tous les <**A.03.12.01.ODP : fréquence**> afin de déterminer si les exigences sont satisfaites

Méthodes et objets d'évaluation potentiels :

Examen

[Sélection parmi les options suivantes : politique et procédures liées à l'évaluation de sécurité et à la surveillance; procédures liées à la planification de l'évaluation de sécurité; plan d'évaluation de la sécurité; rapport d'évaluation de la sécurité; plan de sécurité du système; plan de protection de la vie privée; autres documents ou enregistrements pertinents]

Entrevue

[Sélection parmi les options suivantes : personnel responsable de l'évaluation de sécurité; personnel responsable de la sécurité de l'information et de la protection de la vie privée]

Test

[Sélection parmi les options suivantes : mécanismes liés au soutien des évaluations de sécurité, processus liés à l'élaboration de plans d'évaluation de sécurité ou rapports d'évaluation de sécurité]

Références :

Procédure d'évaluation tirée de la source : CA-02

03.12.02 Plans d'action et des jalons

Confirmer l'exécution des actions suivantes :

A.03.12.02.A.01 : développer un plan d'action et des jalons pour le système afin de consigner les mesures correctives pour corriger les faiblesses ou les lacunes relevées durant l'évaluation de sécurité

A.03.12.02.A.02 : développer un plan d'action et des jalons pour le système afin de réduire ou éliminer les vulnérabilités connues du système

A.03.12.02.B.01 : mettre à jour le plan d'action et les jalons existants en tenant compte des constatations des évaluations de sécurité

A.03.12.02.B.02 : mettre à jour le plan d'action et les jalons existants en tenant compte des constatations des vérifications ou des examens

A.03.12.02.B.03 : mettre à jour le plan d'action et les jalons existants en tenant compte des constatations des activités de surveillance continue

Méthodes et objets d'évaluation potentiels :

Examen

[Sélection parmi les options suivantes : politique et procédures liées à l'évaluation de sécurité et à la surveillance; procédures liées aux plans d'action et aux jalons; plan d'évaluation de sécurité; rapports d'évaluation de sécurité; preuve de l'évaluation de sécurité; plan d'action et jalons; plan de sécurité du système; plan de protection de la vie privée; autres documents ou enregistrements pertinents]

Entrevue

[Sélection parmi les options suivantes : personnel responsable de l'élaboration et de la mise en œuvre des plans d'action et des jalons; personnel responsable de la sécurité de l'information et de la protection de la vie privée]

Test

[Sélection parmi les options suivantes : mécanismes liés à l'élaboration, à la mise en œuvre et au maintien des plans d'action et des jalons]

Références :

Procédure d'évaluation tirée de la source : CA-05

03.12.03 Surveillance continue

Confirmer l'exécution des actions suivantes :

A.03.12.03[01] : élaborer une stratégie de surveillance continue des systèmes

A.03.12.03[02] : mettre en œuvre une stratégie de surveillance continue des systèmes

A.03.12.03[03] : tenir compte de la surveillance en cours dans la stratégie de surveillance continue

A.03.12.03[04] : tenir compte des évaluations de sécurité dans la stratégie de surveillance continue

Méthodes et objets d'évaluation potentiels :

Examen

[Sélection parmi les options suivantes : politique et procédures liées à l'évaluation de sécurité et à la surveillance; stratégie de surveillance continue de l'organisation; stratégie de surveillance continue des systèmes; procédures liées à la surveillance continue du système; procédures liées à la gestion des configurations; rapport d'évaluation de sécurité; rapport d'évaluation de la protection de la vie privée; plan d'action et jalons; enregistrements de surveillance du système; enregistrements de gestion des configurations; analyses des répercussions; rapports d'étape; plans de sécurité du système; plan de protection de la vie privée; autres documents ou enregistrements pertinents]

Entrevue

[Sélection parmi les options suivantes : personnel responsable de la surveillance continue; personnel responsable de la sécurité de l'information et de la protection de la vie privée; administratrices et administrateurs de système]

Test

[Sélection parmi les options suivantes : mécanisme de mise en œuvre de la surveillance continue; mécanismes liés au soutien des mesures d'intervention concernant les résultats qui découlent de l'évaluation et de la surveillance; mécanismes liés au soutien des rapports d'étape sur la sécurité et la protection de la vie privée]

Références :

Procédure d'évaluation tirée de la source : CA-07

03.12.04 Non affecté

Retiré par le NIST.

03.12.05 Échange d'information

ODP :

A.03.12.05.ODP[01] : sélection d'une ou plusieurs options parmi les valeurs de paramètres suivantes : {ententes sur la sécurité des interconnexions; ententes sur la sécurité de l'échange d'information; ententes ou protocoles d'entente; accords d'échange de renseignements; accords sur les niveaux de service; ententes avec les utilisatrices et utilisateurs; accords de non-divulgaration; autres types d'ententes}

A.03.12.05.ODP[02] : définir la fréquence à laquelle il convient de passer en revue et de mettre à jour les ententes

Confirmer l'exécution des actions suivantes :

A.03.12.05.A[01] : approuver l'échange d'information désignée entre le système et d'autres systèmes au moyen de
<A.03.12.05.ODP[01] : valeurs de paramètres sélectionnées>

A.03.12.05.A[02] : gérer l'échange d'information désignée entre le système et d'autres systèmes au moyen de
<A.03.12.05.ODP[01] : valeurs de paramètres sélectionnées>

A.03.12.05.B[01] : documenter, dans le cadre des ententes d'échange, les caractéristiques d'interface de chacun des systèmes

A.03.12.05.B[02] : documenter, dans le cadre des ententes d'échange, les exigences de sécurité et de protection de la vie privée liées à chacun des systèmes

A.03.12.05.B[03] : documenter, dans le cadre des ententes d'échange, les responsabilités liées à chacun des systèmes

A.03.12.05.C[01] : passer en revue les ententes d'échange tous les **<A.03.12.05.ODP[02] : fréquence>**

A.03.12.05.C[02] : mettre à jour les ententes d'échange tous les **<A.03.12.05.ODP[02] : fréquence>**

Méthodes et objets d'évaluation potentiels :**Examen**

[Sélection parmi les options suivantes : politique et procédures liées au contrôle de l'accès; procédures liées aux connexions du système; politique et procédures liées à la protection des systèmes et des communications; ententes sur la sécurité des interconnexions de systèmes; ententes sur la sécurité de l'échange d'information; accords sur les niveaux de service; ententes ou protocoles d'entente; accords d'échange de renseignements; accords de non-divulgence; documents sur la conception du système; architecture d'entreprise; architecture de sécurité; paramètres de configuration du système; plan de sécurité du système; plan de protection de la vie privée; autres documents ou enregistrements pertinents]

Entrevue

[Sélection parmi les options suivantes : personnel responsable de l'élaboration, de la mise en œuvre et de l'approbation des accords sur les interconnexions de systèmes; personnel responsable de la gestion des systèmes auxquels les ententes d'échange s'appliquent; personnel responsable de la sécurité de l'information et de la protection de la vie privée]

Références :

Procédure d'évaluation tirée de la source : CA-03

3.13 Protection des systèmes et des communications

Les contrôles de la famille Protection des systèmes et des communications appuient les activités de surveillance, de contrôle et de protection des systèmes ainsi que les communications internes et externes des systèmes.

03.13.01 Protection des frontières

Confirmer l'exécution des actions suivantes :

A.03.13.01.A[01] : surveiller les communications transmises des interfaces gérées externes au système

A.03.13.01.A[02] : contrôler les communications transmises des interfaces gérées externes au système

A.03.13.01.A[03] : surveiller les communications vers les principales interfaces gérées internes depuis le système

A.03.13.01.A[04] : contrôler les communications vers les principales interfaces gérées internes depuis le système

A.03.13.01.B : mettre en œuvre des sous-réseaux pour les composants de systèmes à accès public qui sont séparés physiquement ou logiquement des réseaux internes

A.03.13.01.C : établir les connexions des systèmes externes seulement au moyen d'interfaces gérées constituées de dispositifs de protection de périmètre organisés conformément à l'architecture de sécurité de l'organisation

Méthodes et objets d'évaluation potentiels :**Examen**

[Sélection parmi les options suivantes : politique et procédures de protection des systèmes et des communications; procédures liées à la protection des frontières; liste des principales frontières internes du système; matériel et logiciels de

protection des frontières; paramètres de configuration du système; architecture de sécurité; enregistrements de vérification du système; documents sur la conception du système; documents sur l'architecture de sécurité d'entreprise; plan de sécurité du système; autres documents ou enregistrements pertinents]

Entrevue

[Sélection parmi les options suivantes : personnel responsable de la protection des frontières; personnel responsable de la sécurité de l'information; développeuses et développeurs de système; administratrices et administrateurs de système]

Test

[Sélection parmi les options suivantes : mécanismes liés à la mise en œuvre des capacités de protection des frontières]

Références :

Procédure d'évaluation tirée de la source : SC-07

03.13.02 Non affecté

Retiré par le NIST.

03.13.03 Non affecté

Retiré par le NIST.

03.13.04 Information dans les ressources système partagées

Confirmer l'exécution des actions suivantes :

A.03.13.04[01] : prévenir le transfert non autorisé d'information par l'intermédiaire de ressources partagées

A.03.13.04[02] : prévenir le transfert non prévu d'information par l'intermédiaire de ressources partagées

Méthodes et objets d'évaluation potentiels :

Examen

[Sélection parmi les options suivantes : politique et procédures de protection des systèmes et des communications; procédures liées à la protection de l'information dans des ressources système partagées; paramètres de configuration du système; enregistrements de vérification du système; documents sur la conception du système; plan de sécurité du système; autres documents ou enregistrements pertinents]

Entrevue

[Sélection parmi les options suivantes : personnel responsable de la sécurité de l'information; développeuses et développeurs de système; administratrices et administrateurs de système]

Test

[Sélection parmi les options suivantes : mécanismes liés à la prévention du transfert non autorisé et non prévu d'information par l'intermédiaire de ressources système partagées]

Références :

Procédure d'évaluation tirée de la source : SC-04

03.13.05 Non affecté

Retiré par le NIST.

03.13.06 Communications réseau – Refus par défaut et autorisation par exception**Confirmer l'exécution des actions suivantes :**

A.03.13.06[01] : refuser par défaut le trafic de communication réseau

A.03.13.06[02] : autoriser à titre exceptionnel le trafic de communication réseau

Méthodes et objets d'évaluation potentiels :**Examen**

[Sélection parmi les options suivantes : politique et procédures de protection des systèmes et des communications; procédures liées à la protection des frontières; documents sur la conception du système; paramètres de configuration du système; enregistrements de vérification du système; plan de sécurité du système; autres documents ou enregistrements pertinents]

Entrevue

[Sélection parmi les options suivantes : personnel responsable de la protection des frontières; personnel responsable de la sécurité de l'information; développeuses et développeurs de système; administratrices et administrateurs de système]

Test

[Sélection parmi les options suivantes : mécanismes liés à la mise en œuvre de la gestion du trafic à proximité des interfaces gérées]

Références :

Procédure d'évaluation tirée de la source : SC-07(05)

03.13.07 Non affecté

Retiré par le NIST.

03.13.08 Confidentialité lors de la transmission et du stockage**Confirmer l'exécution des actions suivantes :**

A.03.13.08[01] : mettre en œuvre des mécanismes cryptographiques afin d'empêcher la divulgation non autorisée d'information désignée durant la transmission

A.03.13.08[02] : mettre en œuvre des mécanismes cryptographiques afin d'empêcher la divulgation non autorisée d'information désignée lors du stockage

Méthodes et objets d'évaluation potentiels :

Examen

[Sélection parmi les options suivantes : politique et procédures de protection des systèmes et des communications; procédures liées à la confidentialité des transmissions; procédures liées à la protection de l'information au repos; documents sur la conception du système; paramètres de configuration du système; documents sur les mécanismes cryptographiques et la configuration connexe; information en stockage dont il faut protéger la confidentialité; enregistrements de vérification du système; plan de sécurité du système; autres documents ou enregistrements pertinents]

Entrevue

[Sélection parmi les options suivantes : personnel responsable de la sécurité de l'information; développeuses et développeurs de système; administratrices et administrateurs de système]

Test

[Sélection parmi les options suivantes : mécanismes de prise en charge ou de mise en œuvre de la confidentialité des transmissions; mécanismes cryptographiques liés à la prise en charge ou à la mise en œuvre de la confidentialité des transmissions; mécanismes de prise en charge ou de mise en œuvre de protection de la confidentialité de l'information en stockage; mécanismes cryptographiques liés à la mise en œuvre de la protection de la confidentialité de l'information en stockage]

Références :

Procédures d'évaluation tirées de la source : SC-08, SC-08(01), SC-28 et SC-28(01)

03.13.09 Déconnexion du réseau

ODP :

A.03.13.09.ODP : définir la période d'inactivité après laquelle il convient de mettre fin à la connexion réseau associée à la session de communication

Confirmer l'exécution des actions suivantes :

A.03.13.09 : mettre fin à la connexion réseau associée à la session de communication à la fin de la session ou après <**A.03.13.09.ODP** : délai> d'inactivité

Méthodes et objets d'évaluation potentiels :

Examen

[Sélection parmi les options suivantes : politique et procédures de protection des systèmes et des communications; procédures liées à la déconnexion du réseau; documents sur la conception du système; paramètres de configuration du système; enregistrements de vérification du système; plan de sécurité du système; autres documents ou enregistrements pertinents]

Entrevue

[Sélection parmi les options suivantes : personnel responsable de la sécurité de l'information; développeuses et développeurs de système; administratrices et administrateurs de système]

Test

[Sélection parmi les options suivantes : mécanismes de prise en charge ou de mise en œuvre d'une capacité de déconnexion du réseau]

Références :

Procédure d'évaluation tirée de la source : SC-10

03.13.10 Établissement et gestion des clés cryptographiques**ODP :**

A.03.13.10.ODP : définir les exigences liées à la génération, à la distribution, au stockage et à la destruction des clés, ainsi qu'à l'accès à celles-ci

Confirmer l'exécution des actions suivantes :

A.03.13.10[01] : établir les clés cryptographiques dans le système conformément aux exigences de gestion des clés suivantes : **<A.03.13.10.ODP : exigences>**

A.03.13.10[02] : gérer les clés cryptographiques dans le système conformément aux exigences de gestion des clés suivantes : **<A.03.13.10.ODP : exigences>**

Méthodes et objets d'évaluation potentiels :**Examen**

[Sélection parmi les options suivantes : politique et procédures de protection des systèmes et des communications; procédures liées à l'établissement et à la gestion des clés cryptographiques; documents sur la conception du système; paramètres de configuration du système; mécanismes cryptographiques; enregistrements de vérification du système; plan de sécurité du système; autres documents ou enregistrements pertinents]

Entrevue

[Sélection parmi les options suivantes : personnel responsable de l'établissement et de la gestion des clés cryptographiques; personnel responsable de la sécurité de l'information; administratrices et administrateurs de système]

Test

[Sélection parmi les options suivantes : mécanismes de prise en charge ou de mise en œuvre de l'établissement et de la gestion des clés cryptographiques]

Références :

Procédure d'évaluation tirée de la source : SC-12

03.13.11 Protection cryptographique

ODP :

A.03.13.11.ODP : définir les types de cryptographie nécessaires pour protéger la confidentialité de l'information désignée

Confirmer l'exécution des actions suivantes :

A.03.13.11 : mettre en œuvre les types de cryptographie suivants pour protéger la confidentialité de l'information désignée :

<A.03.13.11.ODP : types de cryptographie>

Méthodes et objets d'évaluation potentiels :

Examen

[Sélection parmi les options suivantes : politique et procédures de protection des systèmes et des communications; procédures liées à la protection cryptographique; documents sur la conception du système; paramètres de configuration du système; certificats de validation des modules cryptographiques; liste des modules cryptographiques validés en vertu de la norme FIPS (Federal Information Processing Standards) 140; enregistrements de vérification du système; plan de sécurité du système; autres documents ou enregistrements pertinents]

Entrevue

[Sélection parmi les options suivantes : personnel responsable de la protection cryptographique; personnel responsable de la sécurité de l'information; développeuses et développeurs de système; administratrices et administrateurs de système]

Test

[Sélection parmi les options suivantes : mécanismes de prise en charge ou de mise en œuvre de la protection cryptographique]

Références :

Procédure d'évaluation tirée de la source : SC-13

03.13.12 Applications et dispositifs d'informatique collaborative

ODP :

A.03.13.12.ODP : définir les exceptions pour lesquelles l'activation à distance doit être permise

Confirmer l'exécution des actions suivantes :

A.03.13.12.A : empêcher l'activation à distance des applications et des dispositifs d'informatique collaborative, sauf pour les exceptions suivantes : **<A.03.13.12.ODP : exceptions>**

A.03.13.12.B : indiquer de manière explicite l'utilisation permise pour les utilisatrices et utilisateurs qui se trouvent physiquement à proximité des dispositifs

Méthodes et objets d'évaluation potentiels :**Examen**

[Sélection parmi les options suivantes : politique et procédures de protection des systèmes et des communications; procédures liées à l'informatique collaborative; politique et procédures de contrôle d'accès; paramètres de configuration du système; documents sur la conception du système; enregistrements de vérification du système; plan de sécurité du système; autres documents ou enregistrements pertinents]

Entrevue

[Sélection parmi les options suivantes : personnel responsable de la gestion des dispositifs d'informatique coopérative; personnel responsable de la sécurité de l'information; développeuses et développeurs de système; administratrices et administrateurs de système]

Test

[Sélection parmi les options suivantes : mécanismes de prise en charge ou de mise en œuvre de la gestion de l'activation à distance des dispositifs d'informatique coopérative; mécanismes liés à l'indication de l'utilisation de dispositifs d'informatique coopérative]

Références :

Procédure d'évaluation tirée de la source : SC-15

03.13.13 Code mobile**Confirmer l'exécution des actions suivantes :**

A.03.13.13.A[01] : définir le code mobile acceptable

A.03.13.13.A[02] : définir les technologies de code mobile acceptables

A.03.13.13.B[01] : autoriser l'utilisation du code mobile

A.03.13.13.B[02] : surveiller l'utilisation du code mobile

A.03.13.13.B[03] : contrôler l'utilisation du code mobile

Méthodes et objets d'évaluation potentiels :**Examen**

[Sélection parmi les options suivantes : politique et procédures de protection des systèmes et des communications; procédures liées au code mobile; stratégie et procédures de mise en œuvre du code mobile; liste des codes mobiles et des technologies de code mobile acceptables; enregistrements d'autorisation; enregistrements de surveillance du système; enregistrements de vérification du système; plan de sécurité du système; autres documents ou enregistrements pertinents]

Entrevue

[Sélection parmi les options suivantes : personnel responsable de la gestion du code mobile; personnel responsable de la sécurité de l'information; administratrices et administrateurs de système]

Test

[Sélection parmi les options suivantes : processus liés à l'autorisation, à la surveillance et au contrôle du code mobile; mécanismes de prise en charge ou de mise en place de la gestion du code mobile; mécanismes de prise en charge ou de mise en œuvre de la surveillance du code mobile]

Références :

Procédure d'évaluation tirée de la source : SC-18

03.13.14 Non affecté

Retiré par le NIST.

03.13.15 Authenticité des sessions**Confirmer l'exécution des actions suivantes :**

A.03.13.15 : protéger l'authenticité des sessions de communication

Méthodes et objets d'évaluation potentiels :**Examen**

[Sélection parmi les options suivantes : politique et procédures de protection des systèmes et des communications; procédures liées à l'authenticité des sessions; documents sur la conception du système; paramètres de configuration du système; enregistrements de vérification du système; plan de sécurité du système; autres documents ou enregistrements pertinents]

Entrevue

[Sélection parmi les options suivantes : personnel responsable de la sécurité de l'information; administratrices et administrateurs de système]

Test

[Sélection parmi les options suivantes : mécanismes de prise en charge ou de mise en œuvre de l'authenticité des sessions]

Références :

Procédure d'évaluation tirée de la source : SC-23

03.13.16 Non affecté

Retiré par le NIST.

3.14 Intégrité de l'information et des systèmes

Les contrôles de la famille Intégrité de l'information et des systèmes appuient la protection de l'intégrité des composants du système et des données traitées par le système. L'organisation est ainsi en mesure de faire ce qui suit :

- établir, signaler et corriger rapidement les défauts liés aux données et aux systèmes;
- offrir une protection contre les programmes malveillants;
- surveiller les alertes et les avis de sécurité du système;
- intervenir de manière appropriée.

03.14.01 Correction des défauts

ODP :

A.03.14.01.ODP[01] : définir la période durant laquelle il convient d'installer les mises à jour logicielles de sécurité appropriées des logiciels suivant leur date de publication

A.03.14.01.ODP[02] : définir la période durant laquelle il convient d'installer les mises à jour micrologicielles de sécurité appropriées des logiciels suivant leur date de publication

Confirmer l'exécution des actions suivantes :

A.03.14.01.A[01] : relever les défauts du système

A.03.14.01.A[02] : signaler les défauts du système

A.03.14.01.A[03] : corriger les défauts du système

A.03.14.01.B[01] : installer les mises à jour de sécurité des logiciels dans les <**A.03.14.01.ODP[01]** : délai> suivant leur diffusion

A.03.14.01.B[02] : installer les mises à jour de sécurité des micrologiciels dans les <**A.03.14.01.ODP[02]** : délai> suivant leur diffusion

Méthodes et objets d'évaluation potentiels :

Examen

[Sélection parmi les options suivantes : politique et procédures d'intégrité de l'information et du système; procédures d'atténuation des défauts; procédures de gestion des configurations; liste des récentes mesures d'atténuation des failles de sécurité informatique prises sur le système; liste des défauts et des vulnérabilités susceptibles de toucher le système; résultats des tests découlant de l'installation des mises à jour logicielles et micrologicielles effectuées pour corriger les défauts du système; enregistrements d'installation et de contrôle des changements pour les mises à jour de sécurité des logiciels et des micrologiciels; plan de sécurité du système; plan de protection de la vie privée; autres documents et enregistrements pertinents]

Entrevue

[Sélection parmi les options suivantes : personnel responsable de l'installation, de la configuration ou de la maintenance du système; personnel responsable de l'atténuation des défauts; personnel responsable de la gestion des configurations;

personnel responsable de la sécurité de l'information et de la protection de la vie privée; administratrices et administrateurs de système]

Test

[Sélection parmi les options suivantes : processus d'identification, de signalement et de correction des défauts du système; processus d'installation des mises à jour des logiciels et des micrologiciels; mécanismes de prise en charge ou de mise en œuvre du signalement et de la correction des défauts du système; mécanismes de prise en charge ou de mise en œuvre des tests visant les mises à jour des logiciels et des micrologiciels]

Références :

Procédure d'évaluation tirée de la source : SI-02

03.14.02 Protection contre les programmes malveillants

ODP :

A.03.14.02.ODP : définir la fréquence à laquelle les mécanismes de protection contre les programmes malveillants procèdent à des analyses

Confirmer l'exécution des actions suivantes :

A.03.14.02.A[01] : mettre en œuvre des mécanismes de protection contre les programmes malveillants aux points d'entrée et de sortie du système pour détecter le code malveillant

A.03.14.02.A[02] : mettre en œuvre des mécanismes de protection contre les programmes malveillants aux points d'entrée et de sortie du système pour éradiquer le code malveillant

A.03.14.02.B : mettre à jour les mécanismes de protection contre les programmes malveillants dès que de nouvelles versions sont disponibles, conformément à la politique et aux procédures de gestion des configurations

A.03.14.02.C.01[01] : configurer les mécanismes de protection contre les programmes malveillants de manière à effectuer les analyses du système tous les **<A.03.14.02.ODP : fréquence>**

A.03.14.02.C.01[02] : configurer les mécanismes de protection contre les programmes malveillants de manière à effectuer des analyses en temps réel des fichiers de sources externes aux points d'extrémité ou aux points d'entrée et de sortie du système lors de leur téléchargement, de leur ouverture ou de leur exécution

A.03.14.02.C.02 : configurer les mécanismes de protection contre les programmes malveillants de manière à bloquer ou à mettre en quarantaine le code malveillant ou à entreprendre d'autres mesures d'atténuation afin d'intervenir lors de la détection de code malveillant

Méthodes et objets d'évaluation potentiels :

Examen

[Sélection parmi les options suivantes : politique et procédures d'intégrité de l'information et du système; politique et procédures de gestion des configurations; procédures de protection contre les programmes malveillants; enregistrements des mises à jour de la protection contre les programmes malveillants; documents sur la conception du système; paramètres

de configuration du système; résultats des analyses des mécanismes de protection contre les programmes malveillants; enregistrement des actions amorcées par les mécanismes de protection contre les programmes malveillants afin d'intervenir lors de la détection de code malveillant; enregistrements de vérification du système; plan de sécurité du système; autres documents ou enregistrements pertinents]

Entrevue

[Sélection parmi les options suivantes : personnel responsable de la protection contre les programmes malveillants; personnel responsable de l'installation, de la configuration ou de la maintenance du système; personnel responsable de la sécurité de l'information; administratrices et administrateurs de système]

Test

[Sélection parmi les options suivantes : processus pour l'utilisation, la mise à jour et la configuration des mécanismes de protection contre les programmes malveillants; processus de traitement des faux positifs résultant de la détection et des répercussions possibles; mécanismes de prise en charge ou de mise en œuvre, d'utilisation, de mise à jour et de configuration des mécanismes de protection contre les programmes malveillants; mécanismes de prise en charge ou de mise en œuvre de l'analyse du code malveillant et de l'exécution des actions subséquentes]

Références :

Procédure d'évaluation tirée de la source : SI-03

03.14.03 Alertes, avis et directives de sécurité

Confirmer l'exécution des actions suivantes :

A.03.14.03.A : recevoir régulièrement des alertes, des avis et des directives de sécurité concernant les systèmes de la part des organisations externes

A.03.14.03.B[01] : générer les alertes, les avis et les directives de sécurité internes, au besoin

A.03.14.03.B[02] : diffuser les alertes, les avis et les directives de sécurité internes, au besoin

Méthodes et objets d'évaluation potentiels :

Examen

[Sélection parmi les options suivantes : politique et procédures d'intégrité de l'information et des systèmes; procédures liées aux alertes, aux avis et aux directives de sécurité; enregistrements des alertes et des avis de sécurité; plan de sécurité du système; autres documents ou enregistrements pertinents]

Entrevue

[Sélection parmi les options suivantes : personnel responsable des alertes et des avis de sécurité; personnel assurant la mise en œuvre, l'exploitation, le maintien et l'utilisation du système; membres du personnel, éléments organisationnels ou organisations externes à qui les alertes, les avis et les directives de sécurité sont diffusés; personnel responsable de la sécurité de l'information; administratrices et administrateurs de système]

Test

[Sélection parmi les options suivantes : processus liés à la définition, à la réception, à la génération et à la diffusion et au respect des alertes, des avis et des directives de sécurité; mécanismes de prise en charge ou de mise en œuvre des directives de sécurité; mécanismes de prise en charge ou de mise en œuvre de la définition, de la réception, de la génération et de la diffusion des alertes, des avis et des directives de sécurité]

Références :

Procédure d'évaluation tirée de la source : SI-05

03.14.04 Non affecté

Retiré par le NIST.

03.14.05 Non affecté

Retiré par le NIST.

03.14.06 Surveillance des systèmes**Confirmer l'exécution des actions suivantes :**

A.03.14.06.A.01[01] : surveiller le système pour détecter les attaques

A.03.14.06.A.01[02] : surveiller le système pour détecter les indicateurs d'attaques potentielles

A.03.14.06.A.02 : surveiller le système pour détecter les connexions non autorisées

A.03.14.06.B : détecter les utilisations non autorisées du système

A.03.14.06.C[01] : surveiller le trafic de communications entrant pour détecter toute activité ou condition inhabituelle ou non autorisée

A.03.14.06.C[02] : surveiller le trafic de communications sortant pour détecter toute activité ou condition inhabituelle ou non autorisée

Méthodes et objets d'évaluation potentiels :**Examen**

[Sélection parmi les options suivantes : politique et procédures d'intégrité de l'information et des systèmes; procédures liées aux techniques et aux outils de surveillance du système; stratégie de surveillance continue; schéma ou plan de l'installation; documents sur la conception du système; emplacements dans le système où les dispositifs de surveillance seront déployés; paramètres de configuration du système; protocoles du système; enregistrements de vérification du système; plan de sécurité du système; autres documents ou enregistrements pertinents]

Entrevue

[Sélection parmi les options suivantes : personnel responsable de l'installation, de la configuration ou de la maintenance du système; personnel responsable de la surveillance des systèmes; personnel responsable de la détection d'intrusion; personnel responsable de la sécurité de l'information; administratrices et administrateurs de système]

Test

[Sélection parmi les options suivantes : processus liés à la détection d'intrusion et à la surveillance des systèmes; mécanismes de prise en charge ou de mise en œuvre des capacités de surveillance des systèmes; mécanismes de prise en charge ou de mise en œuvre des capacités de détection d'intrusion et de surveillance des systèmes; mécanismes de prise en charge ou de mise en œuvre de la surveillance du trafic de communications entrant et sortant]

Références :

Procédures d'évaluation tirées de la source : SI-04 et SI-04(04)

03.14.07 Non affecté

Retiré par le NIST.

03.14.08 Gestion et conservation de l'information**Confirmer l'exécution des actions suivantes :**

A.03.14.08[01] : gérer l'information désignée au sein du système conformément aux lois, aux décrets, aux directives, à la réglementation, aux politiques, aux normes, aux lignes directrices et aux exigences opérationnelles applicables

A.03.14.08[02] : conserver l'information désignée au sein du système conformément aux lois, aux décrets, aux directives, à la réglementation, aux politiques, aux normes, aux lignes directrices et aux exigences opérationnelles applicables

A.03.14.08[03] : gérer les sorties d'information désignée du système conformément aux lois, aux décrets, aux directives, à la réglementation, aux politiques, aux normes, aux lignes directrices et aux exigences opérationnelles applicables

A.03.14.08[04] : conserver les sorties d'information désignée du système conformément aux lois, aux décrets, aux directives, à la réglementation, aux politiques, aux normes, aux lignes directrices et aux exigences opérationnelles applicables

Méthodes et objets d'évaluation potentiels :**Examen**

[Sélection parmi les options suivantes : politique et procédures d'intégrité de l'information et des systèmes; lois, décrets, directives, politiques, réglementation, normes et exigences opérationnelles applicables à la gestion et à la conservation de l'information; politique de conservation et de disposition des documents; procédures liées à la conservation et à la disposition des documents; politique de traitement des renseignements personnels; politique de protection des supports; procédures de protection des supports; conclusions des vérifications; plan de sécurité du système; plan de protection de la vie privée; plan du programme de protection de la vie privée; inventaire des renseignements personnels; documents sur l'EFVP et l'évaluation des risques d'atteinte à la vie privée; autres documents ou enregistrements pertinents]

Entrevue

[Sélection parmi les options suivantes : personnel responsable de la gestion, de la conservation et de la disposition de l'information et des documents; personnel responsable de la sécurité de l'information et de la protection de la vie privée; administratrices et administrateurs de système]

Test

[Sélection parmi les options suivantes : processus liés à la gestion, à la conservation et à la disposition de l'information; mécanismes de prise en charge ou de mise en œuvre de la gestion, de la conservation et de la disposition de l'information]

Références :

Procédure d'évaluation tirée de la source : SI-12

3.15 Planification

Les contrôles et les activités de la famille Planification sont liés à l'élaboration, à la documentation, à la mise à jour et à la mise en œuvre des plans de sécurité et de protection de la vie privée pour les systèmes organisationnels. Ces plans décrivent les contrôles et les activités de sécurité et de protection de la vie privée en place ou planifiés pour les systèmes. Ils intègrent également les règles de conduite pour les personnes ayant accès aux systèmes.

03.15.01 Politique et procédures

ODP :

A.03.15.01.ODP : définir la fréquence à laquelle il convient de passer en revue et de mettre à jour la politique et les procédures afin de répondre aux exigences de sécurité

Confirmer l'exécution des actions suivantes :

A.03.15.01.A[01] : élaborer et documenter les politiques nécessaires afin de satisfaire les exigences de sécurité pour la protection de l'information désignée

A.03.15.01.A[02] : diffuser au personnel ou aux rôles de l'organisation les politiques nécessaires afin de satisfaire les exigences de sécurité pour la protection de l'information désignée

A.03.15.01.A[03] : élaborer et documenter les procédures nécessaires afin de satisfaire les exigences de sécurité pour la protection de l'information désignée

A.03.15.01.A[04] : diffuser au personnel ou aux rôles de l'organisation les procédures nécessaires afin de satisfaire les exigences de sécurité pour la protection de l'information désignée

A.03.15.01.B[01] : passer en revue les politiques et les procédures tous les **<A.03.15.01.ODP : fréquence>**

A.03.15.01.B[02] : mettre à jour les politiques et les procédures tous les **<A.03.15.01.ODP : fréquence>**

Méthodes et objets d'évaluation potentiels :

Examen

[Sélection parmi les options suivantes : politiques et procédures de sécurité liées à la protection de l'information désignée; résultats des vérifications; plan de sécurité du système; plan de protection de la vie privée; autres documents ou enregistrements pertinents]

Entrevue

[Sélection parmi les options suivantes : personnel responsable de la sécurité de l'information et de la protection de la vie privée]

Références :

Procédures d'évaluation tirées de la source : AC-01, AT-01, AU-01, CA-01, CM-01, IA-01, IR-01, MA-01, MP-01, PE-01, PL-01, PS-01, RA-01, SA-01, SC-01, SI-01 et SR-01

03.15.02 Plan de sécurité du système

ODP :

A.03.15.02.ODP : définir la fréquence à laquelle il convient de passer en revue et de mettre à jour le plan de sécurité du système

Confirmer l'exécution des actions suivantes :

A.03.15.02.A.01 : élaborer un plan de sécurité du système qui décrit les composants constitutifs du système

A.03.15.02.A.02 : élaborer un plan de sécurité du système qui décrit les types d'informations traitées, stockées et transmises par le système

A.03.15.02.A.03 : élaborer un plan de sécurité du système qui décrit les menaces particulières pour le système qui sont préoccupantes pour l'organisation

A.03.15.02.A.04 : élaborer un plan de sécurité du système qui décrit l'environnement opérationnel du système ainsi que les dépendances ou les connexions à d'autres systèmes ou à d'autres composants du système

A.03.15.02.A.05 : élaborer un plan de sécurité du système qui donne une vue d'ensemble des exigences de sécurité

A.03.15.02.A.06 : élaborer un plan de sécurité du système qui décrit les mesures de protection en place ou prévues pour répondre aux exigences de sécurité

A.03.15.02.A.07 : élaborer un plan de sécurité du système qui identifie les personnes qui assument des rôles et des responsabilités liés au système

A.03.15.02.A.08 : élaborer un plan de sécurité du système qui contient d'autres renseignements pertinents nécessaires à la protection de l'information désignée

A.03.15.02.B[01] : passer en revue le plan de sécurité du système tous les <**A.03.15.02.ODP : fréquence**>

A.03.15.02.B[02] : mettre à jour le plan de sécurité du système tous les <**A.03.15.02.ODP : fréquence**>

A.03.15.02.C : protéger le plan de sécurité du système contre les divulgations non autorisées

Méthodes et objets d'évaluation potentiels :

Examen

[Sélection parmi les options suivantes : politique et procédures de planification de la sécurité; procédures liées à l'élaboration et à la mise en œuvre du plan de sécurité et de protection de la vie privée du système; procédures liées aux examens et aux mises à jour du plan de sécurité et de protection de la vie privée du système; architecture d'entreprise; plan de sécurité du système; plan de protection de la vie privée; enregistrements des examens et des mises à jour du plan de sécurité et de protection de la vie privée du système; évaluations des risques; résultats des évaluations des risques; documents sur l'architecture et la conception de la sécurité; autres documents ou enregistrements pertinents]

Entrevue

[Sélection parmi les options suivantes : personnel responsable de la planification et de la mise en œuvre de la sécurité du système; développeuses et développeurs de système; personnel responsable de la sécurité de l'information et de la protection de la vie privée]

Test

[Sélection parmi les options suivantes : processus liés à l'élaboration, à l'examen, à la mise à jour et à l'approbation du plan de sécurité et de protection de la vie privée du système]

Références :

Procédure d'évaluation tirée de la source : PL-02

03.15.03 Règles de conduite

ODP :

A.03.15.03.ODP : définir la fréquence à laquelle il convient de passer en revue et de mettre à jour les règles de conduite

Confirmer l'exécution des actions suivantes :

A.03.15.03.A : établir les règles qui décrivent les responsabilités et le comportement attendu en ce qui concerne l'utilisation du système et la protection de l'information désignée

A.03.15.03.B : fournir des règles aux personnes devant accéder au système

A.03.15.03.C : obtenir des personnes devant accéder au système une attestation documentée selon laquelle elles ont lu et compris le document et acceptent de respecter les règles de conduite avant d'obtenir l'accès autorisé à l'information désignée et au système

A.03.15.03.D[01] : passer en revue les règles de conduite tous les **<A.03.15.03.ODP : fréquence>**

A.03.15.03.D[02] : mettre à jour les règles de conduite tous les **<A.03.15.03.ODP : fréquence>**

Méthodes et objets d'évaluation potentiels :**Examen**

[Sélection parmi les options suivantes : politique et procédures de planification de la sécurité et de la protection de la vie privée; règles de conduite exigées des utilisatrices et utilisateurs du système; attestations signées des règles de conduite; enregistrements des examens et des mises à jour des règles de conduite; plan de sécurité du système; plan de protection de la vie privée; ententes d'échange de renseignements; autres documents ou enregistrements pertinents]

Entrevue

[Sélection parmi les options suivantes : personnel responsable d'établir, de passer en revue et de mettre à jour les règles de conduite; personnel responsable de la formation et de la sensibilisation; personnel responsable de la formation basée sur les rôles; utilisatrices et utilisateurs autorisés du système ayant signé les règles de conduite; personnel responsable de la sécurité de l'information et de la protection de la vie privée]

Test

[Sélection parmi les options suivantes : processus liés à l'établissement, à l'examen, à la diffusion et à la mise à jour des règles de conduite; mécanismes de prise en charge ou de mise en œuvre de l'établissement, de la diffusion, de l'examen et de la mise à jour des règles de conduite]

Références :

Procédure d'évaluation tirée de la source : PL-04

3.16 Acquisition des systèmes et des services

Les contrôles de la famille Acquisition des systèmes et des services s'appliquent à la passation de marchés pour l'acquisition des produits et des services nécessaires afin de soutenir la mise en œuvre et l'exploitation des systèmes organisationnels. Ils permettent de s'assurer que des ressources suffisantes sont affectées à la protection des systèmes organisationnels et ils appuient les processus relatifs au cycle de développement des systèmes qui intègrent des considérations de sécurité.

03.16.01 Principes d'ingénierie de la sécurité des systèmes

ODP :

A.03.16.01.ODP : définir les principes d'ingénierie de la sécurité des systèmes à appliquer au développement ou à la modification du système et des composants du système

Confirmer l'exécution des actions suivantes :

A.03.16.01 : appliquer <**A.03.16.01.ODP : principes d'ingénierie de la sécurité des systèmes**> au développement ou à la modification du système ou des composants du système

Méthodes et objets d'évaluation potentiels :**Examen**

[Sélection parmi les options suivantes : politique d'acquisition des systèmes et des services; procédures d'acquisition des systèmes et des services; procédures liées aux principes d'ingénierie de la sécurité utilisés dans le cadre du développement et de la modification du système; documents sur la conception du système; exigences de sécurité et de protection de la vie privée et spécifications du système; plan de sécurité du système; plan de protection de la vie privée; autres documents ou enregistrements pertinents]

Entrevue

[Sélection parmi les options suivantes : personnel responsable de l'acquisition et de la passation de marché; personnel responsable de la sécurité de l'information et de la protection de la vie privée; personnel responsable du développement et de la modification du système; développeuses et développeurs de système]

Test

[Sélection parmi les options suivantes : processus liés à l'application des principes d'ingénierie de la sécurité dans le cadre du développement et de la modification du système; mécanismes liés à l'application des principes d'ingénierie de la sécurité dans le cadre du développement et de la modification du système]

Références :

Procédure d'évaluation tirée de la source : SA-08

03.16.02 Composants de systèmes non pris en charge**Confirmer l'exécution des actions suivantes :**

A.03.16.02.A : remplacer les composants du système lorsqu'ils ne sont plus pris en charge par les développeuses, les développeurs, les fournisseurs ou les fabricants

A.03.16.02.B : fournir des options pour l'atténuation des risques ou des solutions de rechange visant à assurer la continuité du soutien des composants non pris en charge si ces composants ne peuvent pas être remplacés

Méthodes et objets d'évaluation potentiels :**Examen**

[Sélection parmi les options suivantes : politique et procédures d'acquisition des systèmes et des services; procédures liées au remplacement ou à l'utilisation continue de composants de systèmes non pris en charge; preuves documentées du remplacement de composants de systèmes non pris en charge; approbations documentées (avec justification) de l'utilisation continue de composants de systèmes non pris en charge; plan de GRCA; plan de sécurité du système; autres documents ou enregistrements pertinents]

Entrevue

[Sélection parmi les options suivantes : personnel responsable de l'acquisition des systèmes et des services; personnel responsable du remplacement des composants; personnel responsable du cycle de développement du système; personnel responsable de la sécurité de l'information]

Test

[Sélection parmi les options suivantes : processus liés au remplacement des composants de systèmes non pris en charge; mécanismes de prise en charge ou de mise en œuvre du remplacement des composants de systèmes non pris en charge]

Références :

Procédure d'évaluation tirée de la source : SA-22

03.16.03 Services de systèmes externes**ODP :**

A.03.16.03.ODP : établir les exigences de sécurité auxquelles les fournisseurs de services des systèmes externes doivent se conformer

Confirmer l'exécution des actions suivantes :

A.03.16.03.A : exiger que les fournisseurs de services de systèmes externes utilisés pour le traitement, le stockage ou la transmission de l'information désignée respectent les exigences de sécurité suivantes : **<A.03.16.03.ODP : exigences de sécurité>**

A.03.16.03.B : définir et documenter les rôles et les responsabilités des utilisatrices et utilisateurs concernant les services de système externe, y compris les responsabilités partagées avec les fournisseurs de services externes

A.03.16.03.C : mettre en œuvre des processus, des méthodes et des techniques pour surveiller la conformité aux exigences de sécurité des fournisseurs de services externes sur une base continue

Méthodes et objets d'évaluation potentiels :**Examen**

[Sélection parmi les options suivantes : politique et procédures d'acquisition des systèmes et des services; procédures liées au contrôle de la conformité des fournisseurs de services externes aux exigences de sécurité; documents relatifs à l'acquisition; contrats; accords sur les niveaux de service; ententes entre les organisations; accords de licence; liste des exigences de sécurité pour les services de fournisseurs externes; résultats des évaluations ou rapports des fournisseurs de services externes; plan de GRCA; plan de sécurité du système; autres documents ou enregistrements pertinents]

Entrevue

[Sélection parmi les options suivantes : personnel responsable de l'acquisition; fournisseurs externes de services de systèmes; personnel responsable de la GRCA; personnel responsable de la sécurité de l'information et de la protection de la vie privée]

Test

[Sélection parmi les options suivantes : processus organisationnels de contrôle de la conformité des fournisseurs de services externes aux contrôles de sécurité et de protection de la vie privée sur une base continue; mécanismes de contrôle de la conformité des fournisseurs de services externes aux contrôles de sécurité et de protection de la vie privée sur une base continue]

Références :

Procédure d'évaluation tirée de la source : SA-09

3.17 Gestion des risques liés à la chaîne d'approvisionnement

Les contrôles de la famille Gestion des risques liés à la chaîne d'approvisionnement appuient l'atténuation des risques de cybersécurité dans toutes les phases de la chaîne d'approvisionnement.

03.17.01 Plan de gestion des risques liés à la chaîne d'approvisionnement

ODP :

A.03.17.01.ODP : définir la fréquence à laquelle il convient de passer en revue et de mettre à jour le plan de GRCA

Confirmer l'exécution des actions suivantes :

A.03.17.01.A[01] : élaborer un plan pour gérer les risques liés à la chaîne d'approvisionnement

A.03.17.01.A[02] : s'assurer que le plan de GRCA aborde les risques associés à la recherche et au développement du système, des composants du système ou des services qui s'y rapportent

A.03.17.01.A[03] : s'assurer que le plan de GRCA aborde les risques associés à la conception du système, des composants du système ou des services qui s'y rapportent

A.03.17.01.A[04] : s'assurer que le plan de GRCA aborde les risques associés à la fabrication du système, des composants du système ou des services qui s'y rapportent

A.03.17.01.A[05] : s'assurer que le plan de GRCA aborde les risques associés à l'acquisition du système, des composants du système ou des services qui s'y rapportent

A.03.17.01.A[06] : s'assurer que le plan de GRCA aborde les risques associés à la livraison du système, des composants du système ou des services qui s'y rapportent

A.03.17.01.A[07] : s'assurer que le plan de GRCA aborde les risques associés à l'intégration du système, des composants du système ou des services qui s'y rapportent

A.03.17.01.A[08] : s'assurer que le plan de GRCA aborde les risques associés à l'exploitation du système, des composants du système ou des services qui s'y rapportent

A.03.17.01.A[09] : s'assurer que le plan de GRCA aborde les risques associés à la maintenance du système, des composants du système ou des services qui s'y rapportent

A.03.17.01.A[10] : s'assurer que le plan de GRCA aborde les risques associés à la disposition du système, des composants du système ou des services qui s'y rapportent

A.03.17.01.B[01] : passer en revue le plan de GRCA tous les <**A.03.17.01.ODP : fréquence**>

A.03.17.01.B[02] : mettre à jour le plan de GRCA tous les <**A.03.17.01.ODP : fréquence**>

A.03.17.01.C: protéger le plan de GRCA contre les divulgations non autorisées

Méthodes et objets d'évaluation potentiels :

Examen

[Sélection parmi les options suivantes : politique et procédures de GRCA; plan de GRCA; politique et procédures d'acquisition des systèmes et des services; procédures d'acquisition des systèmes et des services; procédures liées à la protection de la chaîne d'approvisionnement; procédures liées à la protection du plan de GRCA contre les divulgations non autorisées; procédures liées au cycle de développement du système; procédures liées à l'intégration des exigences de sécurité de l'information dans le cadre du processus d'acquisition; documents relatifs à l'acquisition; accords sur les niveaux de service; contrats liés à l'acquisition du système, des composants du système ou des services qui s'y rapportent; liste des menaces liées à la chaîne d'approvisionnement; liste des mesures de protection contre les menaces liées à la chaîne d'approvisionnement, y compris la recherche et le développement, la conception, la fabrication, l'acquisition, la livraison, l'intégration, l'exploitation, la maintenance et la disposition; ententes et procédures entre les organisations; plan de sécurité du système; plan de protection de la vie privée; plan du programme de protection de la vie privée; autres documents ou enregistrements pertinents]

Entrevue

[Sélection parmi les options suivantes : personnel responsable de l'acquisition; personnel responsable de la GRCA; personnel responsable de la sécurité de l'information et de la protection de la vie privée]

Test

[Sélection parmi les options suivantes : processus organisationnels pour la définition et la documentation du cycle de développement du système (CDS); processus organisationnels pour l'identification des rôles et des responsabilités en matière de CDS; processus organisationnels de l'intégration de la GRCA dans le CDS; mécanismes de prise en charge ou de mise en œuvre du CDS]

Références :

Procédure d'évaluation tirée de la source : SR-02

03.17.02 Stratégies, outils et méthodes d'acquisition

Confirmer l'exécution des actions suivantes :

A.03.17.02[01] : élaborer des stratégies d'acquisition, des outils de passation de marchés et des méthodes d'approvisionnement pour déterminer les risques liés à la chaîne d'approvisionnement

A.03.17.02[02] : élaborer des stratégies d'acquisition, des outils de passation de marchés et des méthodes d'approvisionnement pour contrer les risques liés à la chaîne d'approvisionnement

A.03.17.02[03] : élaborer des stratégies d'acquisition, des outils de passation de marchés et des méthodes d'approvisionnement pour atténuer les risques liés à la chaîne d'approvisionnement

A.03.17.02[04] : mettre en œuvre des stratégies d'acquisition, des outils de passation de marchés et des méthodes d'approvisionnement pour déterminer les risques liés à la chaîne d'approvisionnement

A.03.17.02[05] : mettre en œuvre des stratégies d'acquisition, des outils de passation de marchés et des méthodes d'approvisionnement pour contrer les risques liés à la chaîne d'approvisionnement

A.03.17.02[06] : mettre en œuvre des stratégies d'acquisition, des outils de passation de marchés et des méthodes d'approvisionnement pour atténuer les risques liés à la chaîne d'approvisionnement

Méthodes et objets d'évaluation potentiels :

Examen

[Sélection parmi les options suivantes : politique et procédures de GRCA; plan de GCRA; politique et procédures d'acquisition des systèmes et des services; procédures liées à la protection de la chaîne d'approvisionnement; procédures liées à l'intégration des exigences de sécurité de l'information dans le processus d'acquisition; documents d'invitation à soumissionner; documents relatifs à l'acquisition (y compris les bons de commande); accords sur les niveaux de service; contrats d'acquisition du système, des composants du système ou des services qui s'y rapportent; documents sur les risques déterminés qui pèsent sur la chaîne d'approvisionnement; plans d'atténuation des risques liés à la chaîne d'approvisionnement; documents liés aux programmes de formation, d'apprentissage et de sensibilisation à l'intention du personnel en ce qui concerne les risques liés à la chaîne d'approvisionnement; plan de sécurité du système; plan de protection de la vie privée; autres documents ou enregistrements pertinents]

Entrevue

[Sélection parmi les options suivantes : personnel responsable de l'acquisition; personnel responsable de la GRCA; personnel responsable de la sécurité de l'information et de la protection de la vie privée]

Test

[Sélection parmi les options suivantes : processus liés à la définition et à l'utilisation de stratégies d'acquisition, d'outils de contrats et de méthodes d'approvisionnement sur mesure; mécanismes liés à la mise en œuvre de stratégies d'acquisition, d'outils de contrats et de méthodes d'approvisionnement sur mesure]

Références :

Procédure d'évaluation tirée de la source : SR-05

03.17.03 Exigences et processus de la chaîne d'approvisionnement

ODP :

A.03.17.03.ODP : définir des exigences de sécurité pour offrir une protection contre les risques liés à la chaîne d'approvisionnement pour les systèmes, les composants de systèmes ou les services qui s'y rapportent ainsi que pour limiter les conséquences ou les dommages potentiels associés aux événements de la chaîne d'approvisionnement

Confirmer l'exécution des actions suivantes :

A.03.17.03.A[01] : établir un processus pour relever les faiblesses ou les lacunes dans les éléments et les processus de la chaîne d'approvisionnement

A.03.17.03.A[02] : établir un processus pour corriger les faiblesses ou les lacunes dans les éléments et les processus de la chaîne d'approvisionnement

A.03.17.03.B : appliquer les exigences de sécurité suivantes pour offrir une protection contre les risques liés à la chaîne d'approvisionnement pour les systèmes, les composants de systèmes ou les services système ainsi que pour limiter les conséquences ou les dommages potentiels associés aux événements de la chaîne d'approvisionnement : **<A.03.17.03.ODP : exigences de sécurité>**

Méthodes et objets d'évaluation potentiels :**Examen**

[Sélection parmi les options suivantes : politique et procédures de GRCA; stratégie de GCRA; plan de GRCA; documents relatifs à l'inventaire des systèmes et des composants du système critiques; politique et procédures d'acquisition des systèmes et des services; procédures liées à l'intégration des exigences de sécurité et de protection de la vie privée dans le processus d'acquisition; documents d'invitation à soumissionner; documents relatifs à l'acquisition (y compris les bons de commande); procédures d'expédition et de manutention; enregistrements et documents sur la gestion des configurations; contrats d'acquisition pour les systèmes ou les services; accords sur les niveaux de service; documents relatifs au registre des risques; plan de sécurité du système; plan de protection de la vie privée; autres documents ou enregistrements pertinents]

Entrevue

[Sélection parmi les options suivantes : personnel responsable de l'acquisition; personnel responsable de la sécurité de l'information et de la protection de la vie privée; personnel responsable de la GRCA]

Test

[Sélection parmi les options suivantes : processus liés à la détermination et la correction des lacunes dans les éléments et les processus de la chaîne d'approvisionnement]

Références :

Procédure d'évaluation tirée de la source : SR-03

A.1 Paramètres définis par l'organisation

Cette annexe énumère les paramètres définis par l'organisation (ODP) qui sont inclus dans les exigences de sécurité de la section 3. Les ODP sont énumérés de façon séquentielle en fonction de la famille d'exigences, en commençant par la première exigence contenant un ODP dans la famille Contrôle d'accès (AC) et en terminant par la dernière exigence contenant un ODP dans la famille Gestion des risques liés à la chaîne d'approvisionnement (SR).

Tableau 1 : Paramètres définis par l'organisation

Exigence de sécurité	Paramètre défini par l'organisation
Gestion des comptes A.03.01.01.ODP[01]	Définir la période d'inactivité du compte avant sa désactivation
Gestion des comptes A.03.01.01.ODP[02]	Définir les délais dans lesquels il convient d'informer les gestionnaires de compte, ainsi que le personnel ou les rôles définis, lorsque les comptes ne sont plus requis
Gestion des comptes A.03.01.01.ODP[03]	Définir les délais dans lesquels il convient d'informer les gestionnaires de compte, ainsi que le personnel ou les rôles définis, lorsque des utilisatrices ou utilisateurs ont quitté leur emploi ou ont fait l'objet d'un transfert
Gestion des comptes A.03.01.01.ODP[04]	Définir les délais dans lesquels il convient d'informer les gestionnaires de compte, ainsi que le personnel ou les rôles définis, lorsque des changements sont apportés à l'utilisation du système ou au principe du besoin de savoir
Gestion des comptes A.03.01.01.ODP[05]	Définir la période d'inactivité prévue avant que les utilisatrices et utilisateurs soient tenus de se déconnecter du système
Gestion des comptes A.03.01.01.ODP[06]	Définir les circonstances dans lesquelles les utilisatrices et utilisateurs sont tenus de se déconnecter du système
Droit d'accès minimal A.03.01.05.ODP[01]	Définir les fonctions de sécurité pour un accès autorisé
Droit d'accès minimal A.03.01.05.ODP[02]	Définir l'information pertinente en matière de sécurité pour un accès autorisé
Droit d'accès minimal A.03.01.05.ODP[03]	Définir la fréquence à laquelle il convient d'examiner les droits d'accès attribués aux rôles ou aux classes d'utilisateur
Droit d'accès minimal – Comptes privilégiés A.03.01.06.ODP	Définir le personnel ou les rôles dont les comptes privilégiés devraient être restreints sur le système
Tentatives d'ouverture de session infructueuses A.03.01.08.ODP[01]	Définir le nombre de tentatives d'ouverture de session non valides consécutives par l'utilisatrice ou utilisateur sur une période déterminée

Tentatives d'ouverture de session infructueuses A.03.01.08.ODP[02]	Définir la période durant laquelle il convient de limiter le nombre de tentatives d'ouverture de session non valides consécutives par l'utilisatrice ou utilisateur
Tentatives d'ouverture de session infructueuses A.03.01.08.ODP[03]	Sélection d'une ou plusieurs options parmi les valeurs de paramètres suivantes : {verrouiller automatiquement le compte ou le nœud pendant <A.03.01.08.ODP[04] : délai> ; verrouiller automatiquement le compte et le nœud jusqu'à ce qu'une administratrice ou un administrateur le libère; retarder automatiquement la prochaine invite d'ouverture de session; aviser automatiquement l'administratrice ou administrateur de système; prendre automatiquement une autre mesure}
Tentatives d'ouverture de session infructueuses A.03.01.08.ODP[04]	Définir la période durant laquelle il convient de verrouiller un compte ou un nœud (le cas échéant)
Verrouillage d'appareil A.03.01.10.ODP[01]	Sélection d'une ou plusieurs options parmi les valeurs de paramètres suivantes : {procéder au verrouillage de l'appareil après <A.03.01.10.ODP[02] : délai> d'inactivité; exiger que l'utilisatrice ou utilisateur procède à un verrouillage d'appareil avant de laisser le système sans surveillance}
Verrouillage d'appareil A.03.01.10.ODP[02]	Définir le délai d'inactivité après lequel il convient de procéder à un verrouillage d'appareil
Fin de session A.03.01.11.ODP	Définir les conditions ou les événements déclencheurs qui exigent l'interruption de la session
Utilisation de systèmes externes A.03.01.20.ODP	Définir les exigences de sécurité à respecter sur les systèmes externes avant de permettre aux personnes autorisées de les utiliser ou d'y accéder
Formation et sensibilisation A.03.02.01.ODP[01]	Définir la fréquence à laquelle il convient de fournir une formation sur la sécurité aux utilisatrices et utilisateurs du système après la formation initiale
Formation et sensibilisation A.03.02.01.ODP[02]	Définir les événements qui exigent que les utilisatrices et utilisateurs du système prennent part à une formation sur la sécurité
Formation et sensibilisation A.03.02.01.ODP[03]	Définir la fréquence à laquelle il convient de fournir une formation sur la sécurité aux utilisatrices et utilisateurs du système après la formation initiale
Formation et sensibilisation A.03.02.01.ODP[04]	Définir les événements qui exigent la mise à jour du contenu de la formation sur la sécurité
Formation basée sur les rôles A.03.02.02.ODP[01]	Définir la fréquence à laquelle il convient de fournir une formation en matière de sécurité basée sur les rôles au personnel affecté après la formation initiale

Formation basée sur les rôles A.03.02.02.ODP[02]	Définir les événements qui exigent une formation basée sur les rôles en matière de sécurité
Formation basée sur les rôles A.03.02.02.ODP[03]	Définir la fréquence à laquelle il convient de mettre à jour une formation sur la sécurité basée sur les rôles aux utilisatrices et utilisateurs du système après la formation initiale
Formation basée sur les rôles A.03.02.02.ODP[04]	Définir les événements qui exigent la mise à jour du contenu de la formation basée sur les rôles en matière de sécurité
Journalisation d'événements A.03.03.01.ODP[01]	Définir les types d'événements sélectionnés pour la journalisation dans le système
Journalisation d'événements A.03.03.01.ODP[02]	Définir la fréquence à laquelle il convient de vérifier et de mettre à jour les types d'événements sélectionnés pour la journalisation
Intervention en cas d'échec du processus de journalisation des données de vérification A.03.03.04.ODP[01]	Définir le délai pendant lequel le personnel ou les rôles de l'organisation reçoivent des alertes en cas d'échec d'un processus de journalisation des données de vérification
Intervention en cas d'échec du processus de journalisation des données de vérification A.03.03.04.ODP[02]	Définir les mesures additionnelles à prendre en cas d'échec d'un processus de journalisation des données de vérification
Examen, analyse et rapports des dossiers de vérification A.03.03.05.ODP	Définir la fréquence à laquelle il convient de vérifier et d'analyser les enregistrements de vérification du système
Horodatage A.03.03.07.ODP	Définir la granularité de mesure du temps pour l'horodatage des enregistrements de vérification
Configuration de référence (A.03.04.01.ODP)	Définir la fréquence à laquelle il convient de passer en revue et de mettre à jour la configuration de référence du système
Paramètres de configuration (A.03.04.02.ODP)	Définir les paramètres de configuration pour le système qui cadrent avec le mode le plus rigoureux sur le plan des exigences opérationnelles
Fonctionnalité minimale A.03.04.06.ODP[01]	Définir les fonctions à interdire ou à restreindre
Fonctionnalité minimale A.03.04.06.ODP[02]	Définir les ports à interdire et à restreindre
Fonctionnalité minimale A.03.04.06.ODP[03]	Définir les protocoles à interdire et à restreindre
Fonctionnalité minimale A.03.04.06.ODP[04]	Définir les connexions à interdire et à restreindre

Fonctionnalité minimale A.03.04.06.ODP[05]	Définir les services à interdire et à restreindre
Fonctionnalité minimale A.03.04.06.ODP[06]	Définir la fréquence à laquelle il convient d'examiner le système afin d'établir les fonctions, les ports, les protocoles, les connexions et les services non nécessaires ou non sécurisés
Logiciels autorisés – Autorisation par exception A.03.04.08.ODP	Définir la fréquence à laquelle il convient de passer en revue et de mettre à jour la liste des programmes informatiques autorisés
Inventaire des composants du système A.03.04.10.ODP	Définir la fréquence à laquelle il convient de passer en revue et de mettre à jour l'inventaire des composants du système
Configuration des systèmes et des composants pour des zones à risque élevé (A.03.04.12.ODP[01])	Définir les configurations des systèmes ou des composants de système à remettre aux personnes qui se rendent dans des endroits à risque élevé
Configuration des systèmes et des composants pour des zones à risque élevé (A.03.04.12.ODP[02])	Définir les exigences en matière de sécurité à appliquer aux systèmes ou aux composants de système lorsque les personnes reviennent de voyage
Identification, authentification et réauthentification des utilisatrices et utilisateurs A.03.05.01.ODP	Définir les circonstances ou les situations exigeant une réauthentification
Identification et authentification des dispositifs A.03.05.02.ODP	Définir les dispositifs ou les types de dispositifs à identifier de façon unique et à authentifier avant d'établir une connexion
Gestion des identifiants A.03.05.05.ODP[01]	Définir le délai après lequel il convient de prévenir la réutilisation d'identifiant
Gestion des identifiants A.03.05.05.ODP[02]	Définir les caractéristiques utilisées pour identifier le statut d'une personne
Gestion des mots de passe A.03.05.07.ODP[01]	Définir la fréquence à laquelle il convient de mettre à jour la liste des mots de passe couramment utilisés, attendus ou compromis
Gestion des mots de passe A.03.05.07.ODP[02]	Définir la composition des mots de passe et les règles de complexité
Gestion des authentifiants A.03.05.12.ODP[01]	Définir la fréquence à laquelle il convient de changer ou d'actualiser les authentifiants
Gestion des authentifiants A.03.05.12.ODP[02]	Définir les événements qui déclenchent le changement ou l'actualisation des authentifiants



Surveillance des incidents, signalement des incidents et assistance en cas d'incident A.03.06.02.ODP[01]	Définir le délai après lequel il convient de signaler les incidents suspects à l'équipe d'intervention en cas d'incident de l'organisation
Surveillance des incidents, signalement des incidents et assistance en cas d'incident A.03.06.02.ODP[02]	Définir les autorités à qui l'information liée à un incident doit être signalée
Tests d'intervention en cas d'incident A.03.06.03.ODP	Définir la fréquence à laquelle il convient de tester l'efficacité de la capacité d'intervention en cas d'incident pour le système
Formation sur les interventions en cas d'incident A.03.06.04.ODP[01]	Définir le délai dans lequel la formation sur les interventions en cas d'incident doit être fournie aux utilisatrices et utilisateurs du système
Formation sur les interventions en cas d'incident A.03.06.04.ODP[02]	Définir la fréquence à laquelle il convient de fournir une formation sur l'intervention en cas d'incident aux utilisatrices et utilisateurs du système
Formation sur les interventions en cas d'incident A.03.06.04.ODP[03]	Définir la fréquence à laquelle il convient de passer en revue et de mettre à jour le contenu de la formation sur les interventions en cas d'incident
Formation sur les interventions en cas d'incident A.03.06.04.ODP[04]	Définir les événements qui déclenchent l'examen du contenu de la formation sur les interventions en cas d'incident
Utilisation des supports A.03.08.07.ODP	Définir les types de supports dont l'utilisation est interdite ou soumise à des restrictions
Filtrage de sécurité du personnel A.03.09.01.ODP	Définir les conditions qui exigent un nouveau filtrage de sécurité des personnes
Cessation d'emploi et mutation de personnel A.03.09.02.ODP	Définir les délais dans lesquels il convient de désactiver l'accès au système
Autorisations d'accès physique A.03.10.01.ODP	Définir la fréquence à laquelle il convient de passer en revue la liste d'accès qui fournit les détails quant aux personnes autorisées à y accéder physiquement
Surveillance de l'accès physique A.03.10.02.ODP[01]	Définir la fréquence à laquelle il convient de passer en revue les journaux d'accès physique
Surveillance de l'accès physique A.03.10.02.ODP[02]	Définir les événements ou les indications potentielles d'événement pour lesquels il convient d'examiner les journaux d'accès physique
Autres lieux de travail A.03.10.06.ODP	Définir les exigences de sécurité à employer dans les autres lieux de travail
Évaluation des risques A.03.11.01.ODP	Définir la fréquence à laquelle il convient de mettre à jour l'évaluation des risques
Surveillance et analyse des vulnérabilités A.03.11.02.ODP[01]	Définir la fréquence à laquelle il convient de surveiller les vulnérabilités dans le système



Surveillance et analyse des vulnérabilités A.03.11.02.ODP[02]	Définir la fréquence à laquelle il convient d'analyser les vulnérabilités dans le système
Surveillance et analyse des vulnérabilités A.03.11.02.ODP[03]	Définir les délais d'exécution dans lesquels il convient de corriger les vulnérabilités du système
Surveillance et analyse des vulnérabilités A.03.11.02.ODP[04]	Définir la fréquence à laquelle il convient de mettre à jour les vulnérabilités du système à analyser
Évaluation de sécurité A.03.12.01.ODP	Définir la fréquence à laquelle il convient d'évaluer les exigences de sécurité du système et de l'environnement dans lequel il est exploité
Échange d'information A.03.12.05.ODP[01]	Sélection d'une ou plusieurs options parmi les valeurs de paramètres suivantes : {ententes sur la sécurité des interconnexions; ententes sur la sécurité de l'échange d'information; ententes ou protocoles d'entente; accords sur les niveaux de service; ententes avec les utilisatrices et utilisateurs; accords de non-divulgaration; autres types d'ententes}
Échange d'information A.03.12.05.ODP[02]	Définir la fréquence à laquelle il convient de passer en revue et de mettre à jour les ententes
Déconnexion du réseau A.03.13.09.ODP	Définir la période d'inactivité après laquelle il convient de mettre fin à la connexion réseau associée à la session de communication
Établissement et gestion des clés cryptographiques A.03.13.10.ODP	Définir les exigences liées à la génération, à la distribution, au stockage et à la destruction des clés, ainsi qu'à l'accès à celles-ci
Protection cryptographique A.03.13.11.ODP	Définir les types de cryptographie nécessaires pour protéger la confidentialité de l'information désignée
Applications et dispositifs d'informatique coopérative A.03.13.12.ODP	Définir les exceptions pour lesquelles l'activation à distance doit être permise
Correction des défauts A.03.14.01.ODP[01]	Définir la période durant laquelle il convient d'installer les mises à jour logicielles de sécurité appropriées des logiciels suivant leur date de publication
Correction des défauts A.03.14.01.ODP[02]	Définir la période durant laquelle il convient d'installer les mises à jour micrologicielles de sécurité appropriées des logiciels suivant leur date de publication
Protection contre les codes malveillants (A.03.14.02.ODP)	Définir la fréquence à laquelle les mécanismes de protection contre les programmes malveillants procèdent à des analyses
Politique et procédures A.03.15.01.ODP	Définir la fréquence à laquelle il convient de passer en revue et de mettre à jour les politiques et les procédures afin de mettre en œuvre les exigences de sécurité



Plan de sécurité du système A.03.15.02.ODP	Définir la fréquence à laquelle il convient de passer en revue et de mettre à jour le plan de sécurité du système
Règles de conduite A.03.15.03.ODP	Définir la fréquence à laquelle il convient de passer en revue et de mettre à jour les règles de conduite
Principes d'ingénierie de la sécurité et de la protection de la vie privée A.03.16.01.ODP	Définir les principes d'ingénierie de la sécurité des systèmes à appliquer au développement ou à la modification du système et des composants du système
Services de systèmes externes A.03.16.03.ODP	Établir les exigences de sécurité auxquelles les fournisseurs de services des systèmes externes doivent se conformer
Plan de gestion des risques liés à la chaîne d'approvisionnement A.03.17.01.ODP	Définir la fréquence à laquelle il convient de passer en revue et de mettre à jour le plan de gestion des risques liés à la chaîne d'approvisionnement
Exigences et processus de la chaîne d'approvisionnement A.03.17.03.ODP	Définir des exigences de sécurité pour offrir une protection contre les risques liés à la chaîne d'approvisionnement pour les systèmes, les composants de systèmes ou les services qui s'y rapportent ainsi que pour limiter les conséquences ou les dommages potentiels associés aux événements de la chaîne d'approvisionnement

Avant-propos

La présente publication est un document NON CLASSIFIÉ publié avec l'autorisation du dirigeant principal du Centre canadien pour la cybersécurité (Centre pour la cybersécurité). Pour obtenir plus d'information ou suggérer des modifications, veuillez communiquer avec le Centre pour la cybersécurité :

- par courriel : contact@cyber.gc.ca
- par téléphone : [613-949-7048](tel:613-949-7048) ou [1-833-CYBER-88](tel:1-833-CYBER-88)

Date d'entrée en vigueur

Le présent document entre en vigueur le 20 avril 2026.

Historique des révisions

Révision	Modifications	Date
1.	Première version.	20 avril 2026

D97-3/10-171-01-2026F-PDF
ISBN 978-0-660-99557-1