ANNEXE B, APPENDICE B2

QUESTIONNAIRE DE CONTRÔLE DE LA SÉCURITÉ PRIORITIRE
SYSTÈME DE GESTION DES ATHLÈTES
MINISTÈRE DE LA DÉFENSE NATIONALE

Couches de la zone de contrôle	Contrôle	Responsable	Définition de l'ITSG-33	Développement et exemples	Preuves
Zonage	Autorité technique (AT) Gestionnaire de projet et développeurs	AC-4	Quel est le flux d'information au sein du système et entre systèmes interconnectés? Le système doit contrôler le flux d'information au sein du système et entre systèmes interconnectés.	Une description de chaque vue, y compris une description et des preuves de contrôle du flux : par exemple, empêcher la transmission en clair sur Internet de renseignements dont l'exportation est contrôlée, bloquer le trafic externe qui prétend provenir de l'organisation, restreindre les requêtes Web vers Internet qui ne proviennent pas d'un serveur Web mandataire interne et limiter le transfert d'information entre organisations en fonction des structures et du contenu des données.	☐ Vues du système (p. ex., SV-1, SV-2). ☐ Vues des opérations (p. ex., OV-1, OV-5B). ☐ Documents d'architecture de sécurité. ☐ Les vues du système et des opérations doivent présenter les composantes réseau : FW, eCDS (diodes), PEI (passerelles d'échange d'information), mandataire de filtrage du contenu.
	AT Architecture, gestionnaire de projet, analyste des activités (AA)	CA-3	La conception des zones de TI est-elle conforme aux lignes directrices ITSG 22 et 38? Est-elle conforme à la norme CAMDN et aux vues VO-1, VO-5B, VS-1 et VS-2? Décrivez le dispositif de protection des limites utilisé pour établir la connexion directe d'un système de sécurité non classifié à un réseau externe.	Vues du CAMDN, DCAS (document sur la conception de l'architecture des systèmes). Les dispositifs approuvés de protection des limites (p. ex., routeurs, pare-feu) gèrent les communications (les flux d'information) entre les systèmes nationaux de sécurité non classifiés et les réseaux externes. Si les systèmes interconnectés relèvent d'agents autorisés distincts, les organisations peuvent conclure des ententes sur la sécurité des interconnexions ou décrire les caractéristiques de l'interface entre	☐ Évaluation de la sécurité matérielle (ESM)). ☐ Ententes sur la sécurité des interconnexions. ☐ Fichier de configuration du dispositif de protection des limites.

				leurs systèmes dans leurs plans de sécurité respectifs.	
Zonage	Autorité organisationnelle (AO)	PE-3	Dans quel type de zone le système d'information est-il hébergé (zone opérationnelle, de sécurité, restreinte)? Quels types de mesures de protection sont appliquées pour limiter l'accès au système ou à l'emplacement (p. ex., pièce sécurisée avec accès par clé et balayage de carte, alarmes antieffraction, pavé, gardes, etc.). Les dispositifs d'accès physique (clés, combinaisons, etc.) sont-ils sécurisés? Les dispositifs d'accès physique font-ils l'objet de prises d'inventaire, de modifications et de surveillance périodiques? Tenez-vous des registres de vérification des accès physiques? Les visiteurs sont-ils escortés et surveillés lorsqu'ils accèdent à la zone?	Photo ou plan de la zone contrôlée. Preuves d'évaluation adéquate de la sécurité matérielle. Confirmation des zones physiques (p. ex., carte de zonage) et données de registre qui confirment qui a accédé à chaque zone.	☐ Évaluation de la sécurité matérielle (ESM). ☐ Registres de vérification des accès physiques par des membres du personnel et des visiteurs autorisés. ☐ Courriel de l'officier de la sécurité des systèmes d'information (OSSI) de l'unité ou du surveillant de la sécurité de l'unité (SSU) local qui confirme le stockage approprié de clés, de combinaisons, de dispositifs d'accès physique, le changement des clés ou des combinaisons, périodiquement ou en cas de compromission.

Gestion des vulnérabilités	AT Architecture	CM-2	Est-ce qu'une configuration de base est appliquée et tenue à jour? [CM-2] La configuration de base est-elle documentée et officiellement examinée?	Concept d'opération (CONOPS) et DCAS en matière de sécurité. Liste des outils logiciels ou matériels qui surveillent les modifications de la configuration.	☐ Liste du matériel et des logiciels qui forment le système d'information, y compris les paramètres de configuration des principales composantes et applications. ☐ Preuve (capture d'écran) des correctifs appliqués et de la fréquence d'application des correctifs au système d'exploitation et aux applications. ☐ Processus ou outils utilisés pour surveiller les modifications de la configuration. ☐ Preuve que les ports, les protocoles et les services qui ne doivent pas être accessibles aux utilisateurs et aux appareils sont désactivés.
Gestion des vulnérabilités	AT SPC, CORFC, DIIGI	RA-5	Effectue-t-on mensuellement des analyses de vulnérabilité?	Preuve que les analyses sont prévues et effectuées, examens des rapports, communication des résultats, méthodes de détection des défaillances.	☐ Courriel du CORFC concernant l'intégration du système aux services nationaux d'évaluation des vulnérabilités (EVAST). ☐ Rapports d'évaluation de la vulnérabilité. ☐ Résultats des analyses de vulnérabilité.

	AT Développement	SI-2	Comment la correction des lacunes est-elle intégrée au processus de gestion de la configuration?	IPO pour l'établissement de rapports sur les vulnérabilités réelles et les lacunes détectées du système et rapport sur les essais liés aux mesures correctives. Rapport sur le renforcement des plateformes.	☐ Preuve (capture d'écran) de la dernière mise à jour du système antivirus (AV) et de la fréquence des mises à jour. ☐ Preuve (capture d'écran) des correctifs appliqués et de la fréquence d'application des correctifs au système d'exploitation et aux applications.
	AT Architecture	SI-7	Utilise-t-on des outils de vérification de l'intégrité du système? Quelles mesures prend-on si des modifications non autorisées des logiciels, des micrologiciels ou des données sont détectées? Dans le cadre d'un hébergement par SPC ou sur GPNet, s'assurer que la demande de changement 48991 est examinée et que les rapports d'analyse de la vulnérabilité sont conservés et transmis mensuellement aux Services d'analyse des vulnérabilités d'entreprise de SPC et au D Sécur GI.	Architecture du système, registres des outils utilisés. Les mécanismes de vérification de pointe (p. ex., vérifications de la parité, vérifications cycliques de la redondance, hachages cryptographiques) et les outils connexes peuvent automatiquement surveiller l'intégrité des systèmes d'information et des applications hébergées. Les mesures peuvent comprendre ce qui suit, sans s'y limiter : restauration des données et des configurations sur le point de restauration le plus récent, annulation des modifications, applications de sanctions au besoin.	☐ Preuve (captures d'écran, registres) relative aux outils de vérification utilisés (p. ex., signatures numériques, vérifications de la parité, vérifications cycliques de la redondance, hachages cryptographiques). ☐ Confirmation que les sauvegardes des données du système et des utilisateurs sont conservées de manière sécuritaire (p. ex., autre site, stockage RAID, virtualisation). ☐ Preuve relative aux sauvegardes : captures d'écran des fichiers sur le serveur de sauvegarde, date et résultats du dernier exercice de restauration de données.

Couches de la zone de contrôle	Contrôle	Responsable	Définition de l'ITSG-33	Développement et exemples	Preuves
Gestion de l'identité et des comptes	AO, AT Administrateurs de système et administrateurs d'applications	AC-2	Décrire en détail les procédures de gestion des comptes du système. Le système doit utiliser des mécanismes automatisés pour gérer les comptes du système d'information.	Types de comptes, exigences en matière d'autorisations, création, modification, suppression, désactivation, accès minimal, vérification des comptes, etc. L'utilisation de mécanismes automatisés peut comprendre, par exemple, l'envoi automatique de courriels ou de textos pour aviser les gestionnaires de compte de la fin d'emploi ou de la mutation d'un employé, l'utilisation du système d'information pour surveiller l'utilisation des comptes, l'utilisation d'avis par téléphone pour signaler une utilisation atypique de comptes du système. Captures d'écran qui démontrent la mise en œuvre de la gestion des comptes.	☐ Preuves de la méthode de gestion des comptes d'utilisateur, d'administrateur et de système et de gestion des permissions (captures d'écran, p. ex. stratégies de groupe d'Active Directory). Preuve de la configuration des mots de passe, du verrouillage de session, etc. Rôles des utilisateurs conformes aux rôles définis du système. ☐ Saisie d'écran qui démontre que la connexion au compte root n'est pas permise. ☐ Exemples de registres d'ouvertures de sessions par les administrateurs et les utilisateurs. ☐ Preuve (capture d'écran) de l'activation des registres de vérification des comptes. ☐ Courriel de l'OSSI local qui confirme que les registres de vérification sont examinés régulièrement.

	AT Gestionnaire de projet ou analyste des activités	AC-3	Comment le système applique-t-il les autorisations approuvées aux accès en fonction du besoin de connaître?	Matrice CRUD (créer, lire, mettre à jour, supprimer), contrôle d'accès à base de rôles (CABR) de la part du gestionnaire de projet ou de l'analyste des activités Captures d'écran qui démontrent la mise en œuvre des contrôles.	☐ Capture d'écran qui démontre la mise en œuvre dans Active Directory (AD) du CABR et des mécanismes d'application des droits d'accès (listes ou matrices de contrôle d'accès). ☐ Capture d'écran qui démontre l'appartenance aux groupes. d'AD et la configuration des applications en ce qui concerne l'accès fondé sur les groupes d'AD.
Gestion de l'identité et des comptes	AT Développeurs, architecture	AC-6	Comment le système limite-t-il l'accès des utilisateurs privilégiés et des utilisateurs finaux. Comment le système empêche-t-il les utilisateurs non privilégiés d'exécuter des fonctions privilégiées? L'application doit empêcher les utilisateurs non privilégiés d'exécuter des fonctions privilégiées, y compris la désactivation, le contournement ou la modification des mesures de protection et des contre-mesures de sécurité mises en œuvre.	Les organisations utilisent le principe de l'accès minimal pour les tâches particulières et pour les systèmes d'information. Dans le cadre des processus d'un système d'information, cela veut dire que les processus fonctionnent selon l'accès minimal requis pour effectuer les fonctions organisationnelles liées à la mission ou aux activités. Le système d'information empêche les utilisateurs non privilégiés d'exécuter des fonctions privilégiées, y compris la désactivation, le contournement ou la modification des mesures de protection de sécurité mises en œuvre. Preuve de la mise en œuvre. Capture d'écran qui montre la gestion de l'accès.	☐ Preuve (capture d'écran) de l'utilisation de l'accès minimal pour des tâches particulières et les processus du système d'information (démontrer que l'utilisation de comptes privilégiés est limitée à des employés ou à des rôles spécifiques).
	AT Développeurs ou administrateurs de système ou d'application	AC-12	Quelle période d'inactivité entraîne la fermeture de la session d'un utilisateur? Comment le système ferme-t-il la session d'un utilisateur inactif?	Il s'agit de la fermeture de sessions logiques ouvertes par l'utilisateur. Une session logique est lancée lorsqu'un utilisateur (ou un processus qui agit au nom d'un utilisateur) accède au système de l'organisation. On peut fermer une session logique sans fermer les	☐ Capture d'écran qui démontre la fermeture d'une session d'utilisateur après une période prédéfinie d'inactivité.

				sessions réseau. La fermeture d'une session ferme tous les processus associés à la session logique de l'utilisateur, sauf les processus que l'utilisateur (le propriétaire de la session) a créés spécifiquement pour se poursuivre après la fin de la session.	
Gestion de l'identité et des comptes	AT Administrateurs de système et administrateurs d'applications	IA-2	Comme le système identifie-t-il de manière unique et authentifie-t-il les utilisateurs finaux et les appareils? Exige-t-il l'authentification multifacteur? Le cas échéant, le fait-il conformément aux directives de l'ITSP 30.031 V3 du CSTC? Quel niveau d'assurance est mis en œuvre? Une application qui traite de l'information sensible doit mettre en œuvre l'authentification multifacteur pour l'accès réseau à des comptes **privilégiés**.	Les organisations utilisent des mots de passe, des jetons ou la biométrie (ou des combinaisons de ceux-ci dans le cas de l'authentification multifacteur) pour authentifier les utilisateurs. L'authentification multifacteur peut utiliser un certificat logiciel associé à un nom d'utilisateur et un mot de passe. Saisies d'écran de la mise en œuvre.	☐ Preuve (saisie d'écran) de l'identification et de l'authentification unique d'utilisateurs de l'organisation. ☐ Preuve de l'utilisation de comptes AD, de comptes locaux, de l'authentification multifacteur et du protocole SAML. ☐ Changement aux comptes AD, aux comptes locaux, à l'authentification multifacteur et au protocole SAML. ☐ Liste d'échantillons de comptes avec date de création et d'expiration.
	AT Développeurs ou administrateurs de système ou d'application	IA-5	L'identité de l'utilisateur, du groupe, du rôle ou de l'appareil qui reçoit un authentifiant est-elle vérifiée avant la distribution de cet authentifiant? Comment l'organisation s'assure-t-elle que le mécanisme d'authentification est suffisamment robuste pour l'utilisation prévue? Quelles procédures sont établies pour modifier et pour révoquer un	IPO pour modifier ou révoquer un mot de passe, liste de groupes qui ont accès au contenu d'authentifiants, définition de la fréquence de modification des authentifiants de comptes privilégiés génériques, prise en charge des configurations. Les authentifiants peuvent être des mots de passe, des dispositifs cryptographiques, des dispositifs de mots de passe ponctuels, des cartes à puce, etc. Les authentifiants de	☐ Preuve (capture d'écran) des politiques en matière de mots de passe. ☐ Copie des IPO qui décrit la mise en œuvre du contrôle.

			authentifiant (p. ex., un mot de passe)? Qui est autorisé à effectuer ces procédures? Qui est autorisé à consulter le contenu d'un authentifiant? Quelles sont les restrictions minimales relatives à la durée de vie d'un authentifiant? Y a-t-il une actualisation ou une modification automatique d'authentifiants?	dispositifs comprennent les certificats et les mots de passe. Le contenu initial d'un authentifiant est son contenu réel (p. ex., mot de passe initial). Par contre, les exigences en matière de contenu d'un authentifiant comprennent des caractéristiques ou des critères particuliers (p. ex., longueur minimale d'un mot de passe). Le système prend en charge la gestion des authentifiants au moyen de paramètres et de restrictions définis par l'organisation	
Gestion de l'identité et des comptes	AT Développeurs ou administrateurs de système ou d'application (suite)	IA-5 (suite)	(Suite) Quelles mesures de sécurité une personne doit-elle prendre? Les authentifiants de comptes privilégiés génériques (p. ex., superutilisateurs) utilisés en développement sont-ils modifiés avant de passer en production? Sont-ils modifiés selon une fréquence définie? Sont-ils modifiés lorsque la liste d'utilisateurs de ces comptes change?	(Suite) (p. ex., longueur minimale des mots de passe, fenêtre de validation pour les jetons à utilisation ponctuelle, nombre de rejets permis lors de la vérification biométrique). On peut prendre des mesures pour protéger les authentifiants individuels, y compris maintenir la possession des authentifiants, ne pas les partager avec d'autres personnes et signaler immédiatement les authentifiants perdus, volés ou compromis. La gestion des authentifiants comprend la délivrance d'authentifiants pour permettre un accès temporaire et la révocation lorsque l'accès n'est plus requis.	
Prévention des pertes de données	AT, AO Administrateurs de système et administrateurs d'applications	PS-6 / PRNK-1	Y a-t-il une entente en matière d'accès au système? Quelle est la fréquence d'examen, de mise à jour et de nouvelle signature, le cas échéant, de l'entente? Vérifier que l'accès à l'information classifiée qui exige une protection particulière n'est attribué qu'aux	Les ententes relatives à l'accès comprennent les ententes de non-divulgation, les ententes sur l'utilisation acceptable, les règles de comportement et les accords sur les conflits d'intérêts. Les ententes relatives à l'accès signées comprennent une reconnaissance que les personnes ont lu, comprennent et acceptent de respecter les contraintes liées aux systèmes de l'organisation auxquels l'accès est autorisé.	☐ Copie signée du formulaire d'entente sur l'accès. ☐ Processus de validation de la création de comptes, administration du système dans le cas d'un système critique de niveau Secret. Marchandises contrôlées,

			personnes qui répondent aux critères suivants : a) possèdent une autorisation d'accès valide attestée par les responsabilités gouvernementales officielles qui leur ont été assignées; b) répondent aux critères connexes en matière de sécurité du personnel; c) ont lu, compris et signé une entente de non-divulgation.		application du niveau Secret (par exemple, au moyen d'un indicateur d'AD pour les personnes autorisées ou d'un courriel du SSU qui confirme qu'il se porte garant des comptes). WebSTAS ou LVERS avec confirmation des autorisations.
Prévention des pertes de données	AT Plateforme/SPC	MP-2	Que fait l'organisation pour surveiller et limiter l'accès pour les supports amovibles sur le système?	Mise en œuvre d'un ensemble strict de contrôles pour le traitement des supports, tel que décrit dans les ordonnances de sécurité. Systèmes configurés pour désactiver l'utilisation d'appareils mobiles (lecteurs USB, CD/DVD, etc.). Les dispositifs techniques utilisés pour faire le suivi doivent être énumérés.	☐ Preuve (capture d'écran) de la mise en œuvre de mesures de prévention des pertes de données. (p. ex., contrôles relatifs aux supports amovibles, USB pour les applications, données au repos, chiffrement, etc.). ☐ Journaux de l'utilisation de supports amovibles validés au moyen de la liste de supports approuvés ou du gardien (p. ex., journaux Stormshield). ☐ Copie des ordonnances de sécurité qui décrivent la mise en œuvre des mesures relatives aux supports amovibles.
	AT Architecture	SC-7	L'architecture et les applications hébergées peuvent-elles détecter et empêcher l'exfiltration non autorisée de données?	Description des mesures de protection des limites, internes et externes.	☐ Capture d'écran qui démontre les règles de pare-feu qui bloquent les connexions.

					☐ Journaux des systèmes de périphérie : pare-feu, eCDS (diodes), passerelles d'échanges d'information, détection des intrusions sur le réseau, mandataire de filtrage de contenu Web. ☐ Confirmation que les sauvegardes des données du système et des utilisateurs sont conservées de manière sécuritaire (p. ex., autre site, stockage RAID, virtualisation).

Couches de la zone de contrôle	Contrôle	Responsable	Définition de l'ITSG-33	Développement et exemples	Preuves
Prévention des pertes de données	AT, AO Administrateurs de système et administrateurs d'applications	PS-6 / PRNK-1	Y a-t-il une entente en matière d'accès au système? Quelle est la fréquence d'examen, de mise à jour et de nouvelle signature, le cas échéant, de l'entente? Vérifier que l'accès à l'information classifiée qui exige une protection particulière n'est attribué qu'aux personnes qui répondent aux critères suivants : a) possèdent une autorisation d'accès valide attestée par les responsabilités gouvernementales officielles qui leur ont été assignées; b) répondent aux critères connexes en matière de sécurité du personnel; c) ont lu, compris et signé une entente de non-divulgation.	Les ententes relatives à l'accès comprennent les ententes de non-divulgation, les ententes sur l'utilisation acceptable, les règles de comportement et les accords sur les conflits d'intérêts. Les ententes relatives à l'accès signées comprennent une reconnaissance que les personnes ont lu, comprennent et acceptent de respecter les contraintes liées aux systèmes de l'organisation auxquels l'accès est autorisé.	☐ Copie signée du formulaire d'entente sur l'accès. ☐ Processus de validation de la création de comptes, administration du système dans le cas d'un système critique de niveau Secret. Marchandises contrôlées, application du niveau Secret (par exemple, au moyen d'un indicateur d'AD pour les personnes autorisées ou d'un courriel du SSU qui confirme qu'il se porte garant des comptes). WebSTAS ou LVERS avec confirmation des autorisations.
	AT Plateforme/SPC	MP-2	Que fait l'organisation pour surveiller et limiter l'accès pour les supports amovibles sur le système?	Mise en œuvre d'un ensemble strict de contrôles pour le traitement des supports, tel que décrit dans les ordonnances de sécurité. Systèmes configurés pour désactiver l'utilisation d'appareils mobiles (lecteurs USB, CD/DVD, etc.). Les dispositifs techniques utilisés pour faire le suivi doivent être énumérés.	☐ Preuve (capture d'écran) de la mise en œuvre de mesures de prévention des pertes de données. (p. ex., contrôles relatifs aux supports amovibles, USB pour les applications, données au repos, chiffrement, etc.). ☐ Journaux de l'utilisation de supports amovibles validés au moyen de la liste de supports

					approuvés ou du gardien (p. ex., journaux Stormshield). ☐ Copie des ordonnances de sécurité qui décrivent la mise en œuvre des mesures relatives aux supports amovibles.
Prévention des pertes de données	AT Architecture	SC-7	L'architecture et les applications hébergées peuvent-elles détecter et empêcher l'exfiltration non autorisée de données?	Description des mesures de protection des limites, internes et externes.	☐ Capture d'écran qui démontre les règles de pare-feu qui bloquent les connexions. ☐ Journaux des systèmes de périphérie : pare-feu, eCDS (diodes), passerelles d'échanges d'information, détection des intrusions sur le réseau, mandataire de filtrage de contenu Web. ☐ Confirmation que les sauvegardes des données du système et des utilisateurs sont conservées de manière sécuritaire (p. ex., autre site, stockage RAID, virtualisation).

Journaux	AT Développement Architecture	SC-26	Quel type de leurre se trouver sur le système? Quelle est la procédure utilisée lorsqu'une attaque, un balayage ou un incident est détecté?	Mise en place des leurres (p. ex., pots de miel, réseaux leurres, réseaux de déception) pour attirer les adversaires et détourner les attaques des systèmes opérationnels qui appuient les missions et les fonctions de l'organisation. Par exemple, une procédure pourrait comprendre l'analyse d'une ou de plusieurs attaques pour détecter l'attaquant, la méthode utilisée et la fréquence des attaques afin de cibler les interventions. On peut alors corriger le système ou signaler les incidents à qui de droit.	☐ Copies des journaux du système leurre et analyse de ceux-ci, le cas échéant. ☐ Copie de l'IPO qui décrit les mesures à prendre en cas de la détection d'une attaque, d'un balayage ou d'un incident liés aux pots de miel ou aux réseaux leurres.
	AT Développeurs, architecture SPC	SI-3	Décrire les mesures de protection contre les programmes malveillants sur le système (les mesures sont-elles héritées de la plateforme ou du réseau?). Quels mécanismes sont utilisés au cours du développement pour assurer l'utilisation de pratiques sécuritaires de codage d'applications?	Points d'entrée et de sortie, mise à jour de la protection, fréquence des balayages, blocage ou mise en quarantaine, faux positifs. Pratiques de codage sécuritaires.	☐ Preuve de la dernière mise à jour du système antivirus (AV) et de la fréquence des mises à jour. ☐ Preuve de l'utilisation de pratiques sécuritaires de codage.
Journaux	AT Développement Architecture	SI-4	Le système peut-il détecter l'utilisation non autorisée ou malveillante du système d'information?	Système de détection d'intrusion (SDI) et système de prévention d'intrusion (SPI), menaces internes et externes, communications sortantes, exfiltration de données.	☐ Preuve de la mise en place d'un système de surveillance (p. ex., courriel du CORFC ou d'un autre organisme qui assure la surveillance du système, y compris les adresses IP et le serveur DNS du système), cas d'utilisation particuliers (p. ex., compromission au moyen de déni de service distribué ou de cyberattaque

					persistante, sécurité des transmissions, enquêtes internes, intervention et rétablissement). ☐ Copie des journaux de SDI et de SPI ou d'autres logiciels de protection contre les programmes malveillants qui détectent des cas d'utilisation non autorisée du système d'information.
	AO, AT Administrateurs de système, administrateurs d'applications	AU-3	Est-ce que le système produit des dossiers de vérification qui contiennent ce qui suit : type d'événement, heure, source, résultat, identité de la personne associée à l'événement?	Le contenu requis des dossiers de vérification pour répondre aux exigences du contrôle comprennent ce qui suit : horodatage, adresses source et de destination, identificateurs d'utilisateur et de processus, description des événements, indications de réussite ou d'échec, fichiers touchés, règles de contrôle d'accès ou de contrôle de flux invoquées.	☐ Preuves (captures d'écran, journaux) qui montrent qui, quoi, quand et où : nom de l'hôte, nom d'utilisateur, adresse IP, horodatage, action exécutée (p. ex., sudo, mount, accès, copie, suppression).
Journaux	AO, AT Architecture, administrateurs d'applications, DPIA 6	AU-2	Décrivez les événements liés aux applications qui font l'objet d'une piste de vérification qui permet une enquête subséquente.	Accès, modification, suppressions, fréquence des vérifications.	☐ Preuve (capture d'écrans, journaux) de la vérification d'événements réussis ou échoués, par exemple : - changement de mot de passe; - connexions échouées; - accès échoués; - activités privilégiées ou autre accès au niveau du système; - connexions simultanées à partir de différents postes de travail; - lancements de programmes.