CENTRE GOUVERNEMENTAL
DE CYBERDÉFENSE

SA-04

Processus d'acquisition

Juill. 2026

Votre gouvernement

Québec

SA

Acquisition sécurisée des systèmes/services

System and Services

SA-04 — Processus d'acquisition (PaFF)

Énoncés :

Inclure, explicitement ou en référence, les exigences, les descriptions et les critères suivants en utilisant [Sélection (un choix ou plus) : langage contractuel normalisé; {Affectation : langage contractuel défini par l'organisation}] dans le contrat d'acquisition du système, des composants du système ou des services qui s'y rapportent :
a. exigences fonctionnelles de sécurité et de protection de la vie privée
b. exigences en matière de robustesse du mécanisme
c. exigences d'assurance de sécurité et de protection de la vie privée
d. contrôles nécessaires pour satisfaire les exigences de sécurité et de protection de la vie privée
e. exigences liées à la documentation sur la sécurité et la protection de la vie privée
f. exigences liées à la protection de la documentation sur la sécurité et la protection de la vie privée
g. description de l'environnement de développement du système et de l'environnement dans lequel on prévoit exploiter le système
h. affectation de responsabilités ou identification des parties responsables de la sécurité et la protection de la vie privée de l'information et de la gestion des risques liés à la chaîne d'approvisionnement
i. critères d'acceptation

Responsable : Aucun

Discussion :

Les exigences fonctionnelles de sécurité et de protection de la vie privée sont habituellement dérivées des exigences de haut niveau en matière de sécurité et de protection de la vie privée décrites au contrôle SA-02. Les exigences dérivées comprennent les capacités, les fonctions et les mécanismes de sécurité et de protection de la vie privée. Les exigences en matière de robustesse qui s'appliquent aux capacités, aux fonctions et aux mécanismes énoncent le degré d'exactitude, d'achèvement, de résistance au trafiquage ou aux contournements, et de résistance aux attaques directes. Les exigences en matière d'assurance peuvent être indiquées dans l'énoncé des travaux dans le cadre du processus de passation du marché et inclure les processus, les procédures et les méthodologies de développement, ainsi que les données des activités de développement et d'évaluation qui prouvent que la fonctionnalité requise a bien été mise en œuvre et que son mécanisme offre la robustesse nécessaire. La publication Activités de gestion des risques pour la cybersécurité et la vie privée tout au long du cycle de vie des systèmes (ITSP. 10.037) du Centre pour la cybersécurité décrit le processus d'ingénierie des exigences dans le cadre du cycle de vie des systèmes. Les contrôles se veulent une description des mesures et des capacités de protection qu'il convient de mettre en œuvre pour atteindre les objectifs précis de l'organisation sur le plan de la sécurité et de la protection de la vie privée, et tenir compte des exigences en matière de sécurité et de protection de la vie privée des parties prenantes. Les contrôles sont sélectionnés et mis en œuvre de manière à satisfaire les exigences du système et à inclure les responsabilités de l'organisation et celles des développeuses et développeurs. Les contrôles peuvent comprendre les aspects techniques, administratifs, physiques et liés à la protection de la vie privée. Dans certains cas, la sélection et la mise en œuvre d'un contrôle peuvent nécessiter de la part de l'organisation des spécifications additionnelles sous la forme d'exigences dérivées ou de valeurs de paramètres de contrôle instanciés. Les exigences dérivées et les valeurs de paramètres de contrôle peuvent s'avérer nécessaires pour fournir le niveau approprié de détail de mise en œuvre des contrôles pendant le cycle de développement des systèmes. Les exigences liées à la documentation sur la sécurité et la protection de la vie privée portent sur toutes les phases du cycle de développement des systèmes. La documentation fournit aux utilisatrices, aux utilisateurs, aux administratrices et aux administrateurs des conseils sur la mise en œuvre et le fonctionnement des contrôles. Le degré de détail requis dans une telle documentation se fonde sur la catégorisation de la sécurité ou sur le niveau de classification du système, de même que sur l'ampleur de la dépendance à l'égard des capacités, des fonctions ou des mécanismes dont dépendent les organisations pour satisfaire les attentes en matière de réponse aux risques. Les exigences peuvent comprendre les paramètres de configuration imposés qui précisent les fonctions, les ports, les protocoles et les services qui sont autorisés. Les critères d'acceptation visant les systèmes, les composants de systèmes et les services qui s'y rapportent sont définis de la même façon que les critères visant toute acquisition ou tout approvisionnement organisationnels. Les organisations peuvent établir d'autres exigences qui soutiennent la sécurité et les activités afin de tenir compte de leurs responsabilités et de celles de la développeuse ou du développeur, ainsi que des exigences en matière de notification et d'échéanciers aux fins de soutien, de maintenance et de mise à jour.