CENTRE GOUVERNEMENTAL DE CYBERDÉFENSE

SA-11

Évaluations et tests effectués par les développeuses et développeurs

Juill. 2026

Votre gouvernement

Québec

SA

Acquisition sécurisée des systèmes/services

System and Services

SA-11 — Évaluations et tests effectués par les développeuses et développeurs (PaFF)

Énoncés :

Exiger que la développeuse ou le développeur du système, du composant du système ou du service qui s'y rapporte fasse ce qui suit à toutes les phases de postconception du cycle de développement du système de manière à :
a. élaborer et mettre en oeuvre un plan pour les évaluations des contrôles de sécurité et de protection de la vie privée en cours
b. procéder au test ou à l'évaluation [Sélection (un choix ou plus) : unité; intégration; système; régression] tous les [Affectation : fréquence définie par l'organisation] selon [Affectation : profondeur et couverture définies par l'organisation]
c. fournir une preuve de l'élaboration d'un plan d'évaluation et des résultats des tests ou de l'évaluation
d. mettre en oeuvre un processus vérifiable de correction des défauts
e. corriger les défauts relevés au cours des tests et de l'évaluation

Paramètres :

b. à définir par l'organisme; à définir par l'organisme; à définir par l'organisme

Responsable : OP

Discussion :

Des tests et des évaluations confirment que les contrôles requis ont été adéquatement mis en oeuvre, qu'ils fonctionnent selon les attentes, qu'ils permettent d'appliquer la stratégie de sécurité et de protection de la vie privée en vigueur et qu'ils répondent aux exigences de sécurité et de protection de la vie privée établies. L'interconnexion des composants de systèmes ou les changements apportés à ces derniers pourraient influer sur les propriétés de sécurité des systèmes et la vie privée des utilisatrices et utilisateurs. Ces interconnexions ou changements, comme la mise à niveau ou le remplacement d'applications, de systèmes d'exploitation et de micrologiciels, peuvent avoir un effet défavorable sur les contrôles mis en oeuvre précédemment. Une évaluation continue au cours du développement fournit des modalités de test et d'évaluation complémentaires que les développeuses et développeurs peuvent utiliser dans le but de réduire ou d'éliminer les défauts éventuels. Les tests liés à des applications logicielles sur mesure peuvent exiger le recours à des approches, comme l'examen manuel du code, l'examen de l'architecture de sécurité, les tests d'intrusion, ainsi que l'analyse statique, l'analyse dynamique, l'analyse binaire ou une combinaison de ces trois types d'analyse. Les développeuses et développeurs peuvent utiliser les approches d'analyse, ainsi que l'instrumentation de sécurité et les tests à données aléatoires, dans une gamme d'outils et dans le cadre des examens du code source. Les plans d'évaluation de la sécurité et de la protection de la vie privée comprennent les activités que les développeuses et développeurs seront appelés à mener, notamment des analyses, des tests, des évaluations et des examens visant des composants logiciels ou micrologiciels, le degré de rigueur à respecter, la fréquence des tests et des évaluations en cours, ainsi que les types d'artéfacts produits durant ces activités. La profondeur des tests et des évaluations porte sur le degré de rigueur et de détail associé au processus d'évaluation. L'envergure des tests et des évaluations renvoie à la portée (par exemple, le nombre et le type) des artéfacts compris dans le processus d'évaluation. Les contrats contiennent les critères d'acceptation relatifs aux plans d'évaluation de la sécurité et de la protection de la vie privée, les processus de correction des lacunes ainsi que les preuves que les plans et les processus ont été appliqués rigoureusement et en temps opportun. Les méthodes d'examen et de protection des plans d'évaluation, des preuves et de la documentation sont proportionnelles à la catégorie de sécurité ou au niveau de classification du système visé. Les contrats peuvent préciser les exigences relatives à la protection des documents.