CENTRE GOUVERNEMENTAL DE CYBERDÉFENSE

SA-09

Services de systèmes externes

Juill. 2026

Votre gouvernement

Québec

SA

Acquisition sécurisée des systèmes/services

System and Services

SA-09 — Services de systèmes externes (PaFF)

Énoncés :

a. Exiger que les fournisseurs de services de systèmes externes respectent les exigences organisationnelles en matière de sécurité et de protection de la vie privée et aient recours aux contrôles suivants : [Affectation : contrôles définis par l'organisation];
b. Définir et documenter la surveillance organisationnelle, de même que les rôles et responsabilités des utilisatrices et utilisateurs en ce qui a trait aux services de systèmes externes;
c. Mettre en oeuvre sur une base continue des processus, des méthodes et des techniques pour surveiller la conformité aux contrôles des fournisseurs de services externes : [Affectation : méthodes, techniques et processus définis par l'organisation].

Paramètres :

a. à définir par l'organisme en fonction du profil de sécurité issu de la classification de sécurité des données numériques gouvernementales
c. au minimum l'exigence d'un rapport d'auditeur externe au prestataire de services démontrant la mise en place et l'efficacité des mesures de sécurité (ex.: SOC2 type 2, ISO 27001, etc.)

Responsable : OP

Discussion :

Les services de systèmes externes sont fournis par un fournisseur externe et l'organisation n'exerce aucun contrôle direct sur le plan de la mise en oeuvre des contrôles requis ou de l'évaluation de l'efficacité de ces contrôles. Les organisations peuvent établir des relations avec des fournisseurs de services externes de nombreuses façons, y compris au moyen de partenariats, de contrats, d'ententes interorganismes, d'ententes liées aux secteurs d'activités, d'accords de licence, de coentreprises et d'échanges de chaîne d'approvisionnement. La responsabilité en matière de gestion des risques pouvant découler du recours à des services de systèmes externes continue d'incomber aux autorités responsables. Dans le cas des services externes, la chaîne d'approbation exige que les organisations créent et maintiennent un certain niveau de confiance en la capacité de chaque fournisseur participant à une relation client-fournisseur d'assurer une protection adéquate des services rendus. La portée et la nature de cette chaîne d'approbation varient en fonction des relations établies entre les organisations et les fournisseurs externes. Les organisations documentent les bases de la relation d'approbation pour que celle-ci puisse faire l'objet d'une surveillance. La documentation des services de systèmes externes comprend les rôles et responsabilités du gouvernement, des fournisseurs de services et des utilisatrices et utilisateurs terminaux en matière de sécurité, ainsi que tout accord sur les niveaux de service pertinent. Les accords sur les niveaux de service définissent les attentes de rendement pour les contrôles mis en oeuvre, décrivent les résultats mesurables et identifient les exigences en matière de solution et d'intervention pour les situations de non-respect qui ont été relevées.