CENTRE GOUVERNEMENTAL
DE CYBERDÉFENSE

RA-03

Évaluation des risques

Juill. 2026

Votre gouvernement

Québec

RA

Évaluation des risques

Risk Assessment

RA-03 — Évaluation des risques (PaFF)

Énoncés :

a. Mener une évaluation des risques, y compris :
- **1.** identifier les menaces et les vulnérabilités dans le système
- **2.** déterminer la probabilité et l'ampleur estimée des préjudices qui pourraient être associés à l'utilisation, à la divulgation, à l'interruption, à la modification et à l'accès non autorisés ou encore à la destruction du système, de l'information qu'il traite, stocke ou transmet, ou toute information connexe
- **3.** déterminer la probabilité et l'incidence de répercussions négatives sur les individus qui peuvent découler du traitement des renseignements personnels

b. Intégrer les résultats de l'évaluation des risques et les décisions liées à la gestion des risques du point de vue de l'organisation et du processus lié à la mission et aux activités aux évaluations des risques au niveau du système
c. Documenter les résultats de l'évaluation des risques dans [Sélection (un choix) : des plans de sécurité et de protection de la vie privée; un rapport d'évaluation des risques; {Affectation : document défini par l'organisation}]
d. Examiner les résultats de l'évaluation des risques [Affectation : fréquence définie par l'organisation]
e. Communiquer les résultats de l'évaluation des risques aux [Affectation : personnel ou rôles définis par l'organisation]
f. Mettre à jour l'évaluation des risques [Affectation : fréquence définie par l'organisation] ou chaque fois que des changements importants sont apportés au système ou à l'environnement d'exploitation, ou encore lorsque d'autres conditions sont susceptibles d'influer sur l'état de sécurité et de protection de la vie privée du système

Paramètres :

c. rapport d'analyse de risques
d. au moins tous les trois (3) ans ou après tout changement significatif
e. la personne ou l'unité propriétaire de risques, le comité de gestion intégrée des risques (GIR) (CODIR ou comité de gestion)
f. au moins tous les trois (3) ans ou après tout changement significatif

Responsable : OP

Discussion :

Les évaluations des risques devraient prendre en compte les menaces, les vulnérabilités, les probabilités et les répercussions sur les activités et les biens organisationnels, les individus, d'autres organisations et le gouvernement. Les évaluations des risques devraient également considérer les risques provenant des parties externes, ce qui comprend les entrepreneures et entrepreneurs exploitant les systèmes au nom de l'organisation, les personnes accédant aux systèmes de l'organisation, les fournisseurs de services et les sous-traitantes et sous-traitants. Les organisations peuvent effectuer des évaluations des risques à chacun des trois niveaux hiérarchiques de la gestion des risques (c'est-à-dire le niveau organisationnel, le niveau du processus lié à la mission et aux activités ou le niveau du système d'information) ainsi qu'à chacune des phases du cycle de développement des systèmes. Les évaluations peuvent également être effectuées à divers stades du processus de gestion des risques, ce qui comprend la préparation, la catégorisation, la sélection, la répartition, la mise en oeuvre, l'évaluation, l'autorisation et la surveillance des contrôles. L'évaluation des risques est une activité continue réalisée tout au long du cycle de développement des systèmes. Elle peut également aborder l'information liée au système, y compris la conception du système, l'utilisation prévue du système, les résultats des tests et les artéfacts ou l'information liée à la chaîne d'approvisionnement. Les évaluations des risques peuvent jouer un rôle important dans les processus de sélection des contrôles, particulièrement pendant la mise en application des directives de personnalisation et les premières phases de la détermination des capacités.