



CENTRE GOUVERNEMENTAL
DE CYBERDÉFENSE

SR-02

Plan de gestion des risques liés à la chaîne d'approvisionnement

Juill. 2026



Gestion des risques liés à la chaîne d'approvisionnement

Supply Chain Risk Management

SR-02 — Plan de gestion des risques liés à la chaîne d'approvisionnement (PaFF)

Énoncés :

- a. Élaborer un plan pour gérer les risques liés à la chaîne d'approvisionnement associés à la recherche, au développement, à la conception, à la fabrication, à l'acquisition, à la livraison, à l'intégration, à l'exploitation, à la maintenance et à l'élimination des systèmes, des composants de systèmes ou des services qui s'y rapportent [Affectation : systèmes, composants de systèmes ou services désignés par l'organisation]
- b. Passer en revue et mettre à jour le plan de GRCA [Affectation : fréquence définie par l'organisation] ou au besoin pour tenir compte des changements organisationnels, environnementaux ou en matière de menaces
- c. Protéger le plan de GRCA contre les divulgations ou les modifications non autorisées

Responsable : Aucun

Discussion :

La dépendance aux produits, aux systèmes et aux services de fournisseurs externes, ainsi que la nature des relations avec ces fournisseurs, présente un niveau accru de risque pour une organisation. Les menaces pouvant augmenter les risques liés à la sécurité et à la protection de la vie privée incluent la production non autorisée, la falsification, le traficage, le vol, l'insertion de logiciel ou de matériel malveillant et les mauvaises pratiques de fabrication et de développement dans la chaîne d'approvisionnement. Les risques liés à la chaîne d'approvisionnement peuvent être endémiques ou systémiques d'un élément ou d'un composant, d'un système, d'une organisation, d'un secteur ou du gouvernement. La gestion des risques liés à la chaîne d'approvisionnement est une tâche complexe à plusieurs facettes nécessitant des efforts coordonnés au sein d'une organisation afin d'établir des relations de confiance et de communiquer avec les parties prenantes internes et externes. Les activités de GRCA comprennent l'identification et l'évaluation des risques, la détermination des mesures appropriées de réponse aux risques, l'élaboration de plans de GRCA visant à documenter les mesures de réponse et la surveillance du rendement par rapport aux plans. Le plan de GRCA (au niveau du système) vise une mise en œuvre en particulier et fournit la mise en œuvre, les exigences, les contraintes et les implications de la stratégie à ce sujet. Ce plan peut être indépendant ou intégré aux plans de sécurité et de protection de la vie privée du système. Les plans de GRCA portent sur la gestion, la mise en œuvre et la surveillance des contrôles de GRCA ainsi que le développement ou le maintien des systèmes pendant le cycle de développement des systèmes (CDS) à l'appui des fonctions liées à la mission et aux activités de l'organisation. Puisque les chaînes d'approvisionnement peuvent varier considérablement au sein d'une même organisation et d'une organisation à l'autre, les plans de GRCA sont adaptés aux programmes individuels et aux contextes organisationnels et opérationnels. Les plans de GRCA personnalisés posent les bases nécessaires pour déterminer si une technologie, un service, un composant de système ou un système convient aux fins prévues et s'il faut également adapter les contrôles en conséquence. Les plans de GRCA sur mesure aident les organisations à concentrer leurs ressources sur les fonctions les plus critiques de la mission et des activités conformément aux exigences liées à la mission et aux activités, ainsi qu'à l'environnement de risque. Les plans de GRCA comprennent une expression de la tolérance de l'organisation aux risques liés à la chaîne d'approvisionnement, les stratégies ou les contrôles d'atténuation des risques acceptables liés à la chaîne d'approvisionnement, un processus visant à évaluer et à surveiller continuellement les risques liés à la chaîne d'approvisionnement, les approches à adopter pour la mise en œuvre et la communication du plan, une description et une justification des mesures d'atténuation prises relativement aux risques liés à la chaîne d'approvisionnement, et les rôles et responsabilités connexes. Pour finir, les plans de GRCA portent sur les exigences liées au développement de systèmes et de composants de système fiables, sécurisés, résilients et protégeant la protection de la vie privée, ce qui comprend l'application des principes du développement sécurisé mis en œuvre dans le cadre des processus d'ingénierie de la sécurité des systèmes basée sur le cycle de vie (voir le contrôle SA-08).