	National Defence Défense nationale		Retour à la liste des DED

DATA ITEM DESCRIPTION – DESCRIPTION DE DONNÉES

1. TITLE – TITRE	2. IDENTIFICATION NUMBER – NUMÉRO D'IDENTIFICATION
ÉVALUATION DES RISQUES POUR LA SÉCURITÉ	**DED 3.10.5**

3. DESCRIPTION / PURPOSE – DESCRIPTION / OBJET

L'évaluation des risques pour la sécurité vise à documenter l'évaluation des cybervulnérabilités, des vecteurs de menaces, de leur probabilité et de leurs répercussions. Les activités d'évaluation des risques pour la sécurité comprennent la définition de la portée, l'évaluation préliminaire des risques pour la sécurité et l'évaluation complète/finale des risques pour la sécurité. L'Entrepreneur doit appuyer des essais de sécurité indépendants effectués par un organisme approuvé par le Canada dans le cadre d'activités de gestion de la vulnérabilité.
Le présent document traite de l'évaluation préliminaire des risques pour la sécurité et de l'évaluation complète/finale des risques pour la sécurité. La définition de la portée doit être couverte dans la définition de la portée en matière de sécurité du système, LDEC 3.10.4.

4. APPROVAL DATE DATE D'APPROBATION	5. OFFICE OF PRIMARY INTEREST (OPI) BUREAU DE PREMIÈRE RESPONSABILITÉ (BPR)	6. GIDEP APPLICABLE APPLICABLE AU GIDEP
ÀD	Autorité technique (AT) de l'OSAN	S.O.

7. APPLICATION / INTERRELATIONSHIP – APPLICATION / INTERDÉPENDANCE

Consulter la LDEC 3.10.5 et le paragraphe 3.10.1 de l'EDT.
Cette DED énonce les instructions relatives au format et au contenu des données produites dans le contexte des tâches énoncées dans l'EDT pour le fonctionnement et l'entretien du Système d'alerte du Nord.

8. ORIGINATOR – AUTEUR	9. APPLICABLE FORMS – FORMULES PERTINENTES
AT OSAN	AUCUNE.

10. PREPARATION INSTRUCTIONS – INSTRUCTIONS SUR LA PRÉSENTATION DES DONNÉES

10.1 Document source

10.1.1 EDT de F et E du SAN section 3, paragraphe 3.10.5.
10.1.2 Processus d'assurance de la cybermission basé sur les risques.

10.2 Contenu et format

10.2.1. L'évaluation des risques pour la sécurité doit être préparée et livrée selon le format utilisé par L'Entrepreneur.

10.2.2. L'évaluation des risques pour la sécurité doit suivre une approche itérative commençant par une évaluation préliminaire des risques qui décrit, avec un haut niveau, les scénarios de menace et se terminant par une évaluation exhaustive des risques qui détaille les scénarios de menace jusqu'au niveau de la mise en œuvre (affiné en série de tactiques, techniques et procédures [TTP]). L'évaluation préliminaire des risques concerne les vulnérabilités dans l'architecture et la conception ou dans les procédures opérationnelles, tandis que l'évaluation exhaustive des risques doit s'achever par l'identification des vulnérabilités dans la mise en œuvre ainsi que dans les mesures de sécurité existantes.

10.2.3. L'évaluation des risques doit être documentée de manière traçable et itérative afin que les menaces et les vulnérabilités trouvées puissent être retracées en tant que menaces et vulnérabilités et puissent être gérées tout au long du cycle de vie du Système d'alerte du Nord. Par exemple, une mise à jour de l'évaluation des risques peut confirmer qu'une vulnérabilité dans la conception déterminée lors d'une itération antérieure de l'évaluation des risques est réellement exploitable. Au minimum, les éléments suivants doivent être détaillés en utilisant les lignes directrices :
a. Identification et évaluation de l'état de la menace.

b. Identification des scénarios de menace.
c. Caractérisation des mesures de sécurité.
d. Niveau d'évaluation des menaces.

10.2.4. En outre, l'évaluation des risques doit documenter ce qui suit à l'aide des lignes directrices du PAMCR pour l'assurance de la mission cybernétique ou d'autres normes acceptables pour le Canada :
a. Vulnérabilités constatées pour ce qui est du niveau d'ingénierie : exigences, architecture, conception, mise en œuvre ou configuration.
b. Menaces, probabilités, répercussions, risques et décisions connexes. Les vulnérabilités associées doivent être indiquées de pair avec les mesures de sécurité connexes au niveau des exigences, de l'architecture, de la conception, de la mise en œuvre ou de la configuration. Les critères et la méthode d'évaluation utilisés pour déterminer le niveau de menace doivent être précisés.
c. Mesures d'atténuation intégrées aux SSR fonctionnels et de façon hiérarchique, c.-à-d. éléments de système, d'architecture, de conception et de mise en œuvre/configuration.

10.2.5. Le document d'évaluation des risques doit inclure une matrice de vulnérabilité. Au minimum, la matrice de vulnérabilité doit inclure les responsables, les noms ou numéros d'identification des biens connexes, l'architecture ou les éléments de conception connexes ainsi que les mesures d'atténuation applicables et le type de vulnérabilité selon la surface d'attaque (personnel, logique, physique, de détection, indirect [chaîne d'approvisionnement] à l'appui de la prise de décisions. La structure de la matrice de vulnérabilité doit normalement suivre l'architecture système et la hiérarchie de conception. Elle doit reposer sur les rapports de vulnérabilité qui ont été publiés pour les produits existants (p. ex. vulnérabilités et expositions communes) dans le cadre de l'évaluation des vulnérabilités. Dans le cadre de l'évaluation des risques, les vulnérabilités découvertes doivent être ajoutées à cette matrice de vulnérabilité.

10.2.6. La catégorisation de sécurité du produit livrable d'évaluation des risques pour la sécurité doit être effectuée lors de la création du document, car l'évaluation des risques pour la sécurité, ou certaines de ses parties, pourraient être protégées et/ou classifiées. L'étiquetage et le marquage de sécurité, ainsi que la manipulation, l'entreposage et la transmission de l'évaluation des risques pour la sécurité doivent être mis en œuvre conformément aux Ordonnances et directives de sécurité de la Défense nationale (ODSDN). Outre le marquage de sécurité, qui est placé dans l'en-tête et le pied de page de chaque page, un ensemble d'énoncés informatifs sera imprimé sur la couverture, ou la première page du document et, dans certains cas, également sur la page verso (au verso de la page de titre ou de la couverture) selon les besoins. Les sections du document qui sont classifiées peuvent indiquer le niveau de classification de chaque élément numéroté (c.-à-d. en-têtes, paragraphes) en plaçant (sc), (C), (S) ou (TS) avant le texte.

10.2.7. Il incombera à L'Entrepreneur de mener la gestion des changements, tel que décrit ci-dessous :
a. L'évaluation des risques pour la sécurité doit comprendre une section sommaire de l'historique des modifications, qui renferme ce qui suit :
i. Un identifiant clair et unique de la version/révision pour chaque soumission ou nouvelle soumission de l'évaluation des risques pour la sécurité.
ii. Une identification claire des révisions ou des modifications apportées au document par rapport à sa soumission précédente.
iii. Le bien-fondé des révisions et des modifications.
b. Toutes les révisions/modifications mentionnées ci-dessus doivent être clairement définies dans le document à l'aide de la fonction de suivi des modifications appropriée du logiciel de traitement de texte utilisé pour produire le document, par exemple, fonction de « Suivi des modifications » dans Microsoft-Word®, barres latérales, etc.