Gestion des risques

Achat de logiciels
Spécifications des exigences logicielles

Révision 1

20 juin 2022

SGDDI OTT_LSTL nº 6191956

TABLE DES MATIÈRES

REGISTRE DES MODIFICATIONS

Il convient de noter que le registre des modifications comprend d'importantes modifications qui ont été apportées au document, mais que des modifications mineures telles que des corrections de formatage et de grammaire ont pu être omises.

Rév.	Section	Récapitulatif des modifications
1	Généralités	Première révision

Remarque : Les spécifications des exigences logicielles ont été élaborées en fonction de la norme internationale 29148-2018 décrite dans les directives de l'Organisation internationale de normalisation (ISO), la Commission électrotechnique internationale (CEI) et l'Institute of Electrical and Electronics Engineers (IEEE) – Ingénierie du logiciel et des systèmes – Processus du cycle de vie - Ingénierie des exigences

1 INTRODUCTION

1.1 Objectif

1.1.1 L'objectif des spécifications des exigences logicielles est de décrire les exigences techniques d'un logiciel de gestion des risques en vue d'appuyer le ministère de la Défense nationale (MDN).

1.2 Portée

1.2.1 L'objectif du logiciel de gestion des risques est de permettre au MDN de relever, d'évaluer et de suivre les risques et les possibilités liés à l'acquisition et le soutien du matériel, ainsi que d'établir les priorités connexes.

1.2.2 Le logiciel de gestion des risques est un outil de collaboration centralisé conçu pour permettre au MDN et à ses partenaires de gérer divers types de risques et de possibilités, tels que les risques et les possibilités liés aux projets et aux programmes, les risques pour la sécurité, les risques liés à la cybersécurité, les risques pour la sécurité des explosifs et des munitions, les risques liés au matériel naval en service et les risques liés à la navigabilité.

1.3 Sigles et définitions

1.3.1 Les sigles utilisés dans les présentes spécifications des exigences logicielles figurent à l'annexe 1.

1.3.2 Les définitions sont les suivantes :

1.3.2.1 Le système infonuagique à topologie en étoile (ou hub en nuage) est un réseau virtuel qui joue le rôle d'emplacement central pour la gestion de la connectivité externe et des services d'hébergement utilisés par plusieurs charges de travail[1] ou rayons. Au sein du MDN, et dans le contexte de cette tâche, le hub en nuage (également appelé « locataire ») est géré de façon centralisée par l'équipe du Programme interarmées d'informatique en nuage de la Défense (PIIND).

1.3.2.2 Les rayons du hub en nuage désignent des réseaux virtuels qui hébergent des charges de travail et se connectent au hub central à l'aide du peering (appairage) de réseaux virtuels. Au sein du MDN, le rayon du hub en nuage est géré par l'organisation cliente. Dans le contexte de cette tâche, l'entrepreneur devra gérer le rayon du hub en nuage et il sera responsable de la sélection, du déploiement et de la configuration des ressources infonuagiques.

1.3.2.3 Énoncé descriptif : tout énoncé qui n'est pas considéré comme une exigence souhaitable ou une exigence obligatoire est un énoncé descriptif ou un en-tête qui doit être utilisé uniquement dans le contexte de cette tâche.

1.3.2.4 Exigence souhaitable : énoncé d'une exigence qui contient le mot « devrait ».

1.3.2.5 Exigence obligatoire : énoncé d'une exigence qui contient le mot « doit ».

1.3.2.6 Norme ouverte : Norme ouverte : norme mise à la disposition du grand public et élaborée (ou approuvée) et tenue à jour au moyen d'un processus axé sur la collaboration et le consensus.

[1] Réseau défini par logiciel : Réseau en étoile, Microsoft Docs (2021-07-09)

Les normes ouvertes facilitent l'interopérabilité et l'échange de données entre différents produits ou services et sont destinées à une adoption généralisée.

1.4 Références

1.4.1 Spécifications, normes et publications du gouvernement du Canada :

	Référence	Publication	Accessibilité de la spécification, de la norme ou de la publication
[A]	Norme sur l'accessibilité des sites Web	1er août 2011	Lien Internet
[B]	Norme sur la facilité d'emploi des sites Web	27 nov. 2013	Lien Internet
[C]	Lignes directrices sur la gestion du risque d'entreprise de la Défense	26 juin 2018	Lien (intranet)
[D]	Ordonnances et directives de sécurité de la Défense nationale, chapitre 3 – Gestion des risques liés à la sécurité	Version 1.2	Lien (intranet)
[E]	Conseils en matière de sécurité des technologies de l'information 33 (ITSG-33) – Gestion du risque lié à la sécurité des technologies de l'information (TI) : Une méthode axée sur le cycle de vie	1er nov. 2012	Lien Internet
[F]	Manuel de sécurité des explosifs et des munitions C-09-005-001/TS-000, volume 1 – Gestion de programme et sécurité du cycle de vie	1er août 2013	Instruction technique des Forces canadiennes (ITFC)
[G]	Gestion des risques du matériel naval C-23-005-000/AG-002	1er août 2013	(ITFC)
[H]	Ordres de la Marine (OMARs) 3001-0 : Gestion des risques liés au matériel naval en service – politique	13 mai 2021	Lien (intranet)
[J]	Ordres de la Marine (OMARs) 3001-1 : Gestion des risques liés au matériel naval en service – processus	24 avril 2014	Lien (intranet)
[K]	Manuel du système de gestion du matériel naval C-03-005-012/AM-001	11 novembre 2013	(ITFC)
[L]	Manuel de navigabilité technique C-05-005-001/AG-001	1er avril 2019	(ITFC)
[M]	Processus de gestion des risques pour la navigabilité EMT01.003	Version D 14 août 2020	(Document de procédures)
[N]	Modèle d'Avis d'alerte de risque par courriel AEPM-009	14 avril 2016	(Modèle de document)
[O]	Modèle d'Alerte de risque pour la navigabilité AEPM-213	11 juillet 2017	(Modèle de document)
[P]	Journal de suivi des risques de navigabilité AEPM-215	29 mai 2017	(Modèle de document)
[Q]	ITSP.40.111 – Algorithmes cryptographiques pour l'information NON CLASSIFIÉE, PROTÉGÉ A et PROTÉGÉ B	1er août 2016	Lien Internet
[R]	ITSP.40.062 – Conseils sur la configuration sécurisée des protocoles réseau	1er octobre 2020	Lien Internet
[S]	Conseils en matière de sécurité des TI 22 (ITSG-22) – Exigences de base en matière de sécurité pour les zones de sécurité de réseau au sein du gouvernement du Canada	1er juin 2007	Lien Internet
[T]	Conseils en matière de sécurité des TI 38 (ITSG-38) – Établissement des zones de sécurité dans un réseau – Considérations de conception relatives au positionnement des services dans les zones	1er mai 2009	Lien Internet

1.4.2 Autres spécifications, normes et publications :

	Référence	Publication	Accessibilité de la spécification, de la norme ou de la publication
[U]	Projet de sécurité ouvert d'applications Web (OWASP) – Les 10 principaux risques de sécurité dans les applications Web	2021	https://owasp.org/Top10/

1.4.3 En cas de divergence entre le contenu du présent document et les références qui y sont citées, le contenu de ce document a préséance.

2 APERÇU DU PRODUIT

2.1 Mise en contexte du produit

2.1.1 Interfaces utilisateurs

2.1.1.1 Le logiciel de gestion des risques doit être accessible aux utilisateurs finaux par le biais d'un navigateur Web, comme décrit plus en détail à la section 3.3.

2.1.2 Interfaces de communication

2.1.2.1 Le logiciel de gestion des risques doit fournir des interfaces de communication par le biais d'une interface de programmation (API), comme décrit plus en détail à la section 3.4.2.

2.1.3 Interfaces avec les services

2.1.3.1 Le logiciel de gestion des risques doit être entièrement hébergé sur un rayon d'informatique en nuage dans l'environnement du PIIND, comme décrit plus en détail à la section 3.4.1.

2.2 Fonctions du produit

2.2.1 Voici les principales fonctions du logiciel de gestion des risques :

2.2.1.1 Permettre aux utilisateurs de saisir, de suivre et d'évaluer les possibilités et les risques globaux liés aux projets et aux programmes, y compris, mais sans s'y limiter :

2.2.1.1.1 Les éléments de risque et de possibilité liés au projet (réf. [C]);

2.2.1.1.2 Les éléments de risque pour la sécurité (réf. [D]);

2.2.1.1.3 Les éléments de risque liés à la cybersécurité (réf. [E]);

2.2.1.1.4 Les éléments de risque pour la sécurité des explosifs et des munitions (réf. [F]).

2.2.1.2 Permettre aux utilisateurs de saisir, de suivre et d'évaluer les possibilités et les risques globaux liés aux classes/flottes et aux plateformes spécifiques (navires, sous-marins, aéronefs et véhicules), y compris :

2.2.1.2.1 Tous les éléments énumérés à la section 2.2.2.1;

2.2.1.2.2 Les éléments de risque liés au matériel naval en service pour les navires et les sous-marins de la Marine (réf. [H] et [J]);

2.2.1.2.3 Les éléments de risque liés à la navigabilité technique et opérationnelle des produits aéronautiques de l'Aviation royale canadienne (ARC) (réf. [L] et [M]).

2.3 Caractéristiques relatives aux utilisateurs

2.3.1 Voici des exemples d'utilisateurs finaux qui interagiront avec le logiciel de gestion des risques :

2.3.1.1 Gestionnaires de l'ingénierie de première ligne : Ils gèrent la maintenance de première ligne des plateformes (navires, sous-marins, aéronefs et véhicules) et sont chargés de signaler les

risques et les possibilités liés aux systèmes et aux équipements aux autorités opérationnelles (y compris les commandants) en vue de prendre des décisions opérationnelles réfléchies. Ils relèvent généralement les éléments de risque conformément à la réf. [F] (pour tous), aux réf. [H] et [J] (pour la Marine) et à la réf. [L] (pour l'ARC). Ils participent généralement à l'approbation technique des éléments de risque.

2.3.1.2 Autorité opérationnelle et commandants : Ils gèrent l'utilisation opérationnelle des plateformes (navires, sous-marins, aéronefs et véhicules) en vue d'accomplir une mission. Ils participent à l'acceptation opérationnelle des éléments de risque.

2.3.1.3 Gestionnaires de l'ingénierie de deuxième ligne : Ils sont chargés de signaler les risques et les possibilités aux commandants de flottes. Ils participent généralement à l'examen de l'aspect technique des éléments de risque relevés par les gestionnaires d'ingénierie de première ligne et à l'approbation technique des éléments de risque. Ils relèvent généralement les éléments de risque conformément à la réf. [F] (pour tous), aux réf. [H] et [J] (pour la Marine) et à la réf. [L] (pour l'ARC).

2.3.1.4 Gestionnaire du cycle de vie du matériel Ils sont chargés de déterminer et de signaler les risques et les possibilités liés aux systèmes et aux équipements relevant de leur domaine de responsabilité. Ils peuvent jouer le rôle d'autorité technique et d'autorité responsable du système. Ils relèvent généralement les éléments de risque conformément à la réf. [C] (pour tous), aux réf. [H] et [J] (pour la Marine) et aux réf. [L] et [M] (pour l'ARC). Les gestionnaires du matériel du cycle de vie participent à l'approbation technique des éléments de risque.

2.3.1.5 Gestionnaires de programmes de classe (Marine) : Ils gèrent les risques et les possibilités pour une classe de navires ou de sous-marins. Ils ont en général au moins 10 ans d'expérience au sein de la communauté technique navale et possèdent au minimum un diplôme universitaire en sciences ou en ingénierie. Ils relèvent généralement les éléments de risque conformément aux références [C], [H] et [J]. Les gestionnaires de programmes de classe participent à l'acceptation technique et opérationnelle des éléments de risque.

2.3.1.6 Gestionnaires des systèmes d'armes (ARC) : Ils sont l'équivalent dans l'ARC des gestionnaires de programmes de classe, lesquels gèrent une flotte d'aéronefs. Ils relèvent généralement des éléments de risque conformément aux références [C], [L] et [M].

2.3.1.7 Les autorités techniques/opérationnelles et l'autorité d'acceptation des risques du commandement opérationnel (ARC) : Ce sont les personnes qui constituent les organismes de réglementation de l'autorité de navigabilité technique (ANT), de l'autorité de navigabilité opérationnelle (ANO), ainsi que l'autorité d'acceptation des risques du commandement opérationnel. Ils participent généralement à l'acceptation technique et opérationnelle des éléments de risque.

2.3.1.8 Gestionnaires de projet : Ils sont chargés de la gestion des risques et des possibilités liés aux programmes et aux projets (telles que les modifications techniques). Ils relèvent généralement les éléments de risque et de possibilité conformément à la Réf. [C].

2.3.1.9 Officier de la sécurité des systèmes d'information (OSSI) : Ils sont chargés de la gestion des risques et des possibilités liés à la sécurité et aux systèmes d'information. Ils relèvent généralement les éléments de risque conformément aux références [D] et [E].

2.3.1.10 Entrepreneur du soutien en service : Ils sont mandatés par le MDN à fournir des services à l’appui des activités d’acquisition et de soutien du matériel. On peut leur demander de remplir tous les rôles définis plus haut, à l’exception du rôle de l’OSSI. Pour des raisons de sécurité, il est important que les entrepreneurs soient limités à l’accès et à la modification des éléments de risque et de possibilité uniquement dans la mesure où ils sont pertinents pour la portée de leur contrat.

2.4 Limites

2.4.1 (Page intentionnellement laissée en blanc)

2.5 Hypothèses et dépendance

2.5.1 Ces spécifications des exigences logicielles présument que le logiciel de gestion des risques (application et base de données connexe) sera déployé dans un environnement en nuage géré par le MDN.

2.5.2 Ces spécifications des exigences logicielles dépendront des services infonuagiques du MDN, notamment :

2.5.2.1 Les services du Simple Mail Transfer Protocol (SMTP);

2.5.2.2 Les services cryptographiques;

2.5.2.3 Identification de l’utilisateur et autorisation d’accès (par le biais d’un répertoire actif).

2.6 Répartition des exigences

2.6.1 (Page intentionnellement laissée en blanc)

3 EXIGENCES

3.1 Fonctions

3.1.1 Accéder au logiciel de gestion des risques

3.1.1.1 Le logiciel de gestion des risques doit disposer d’une page d’accueil offrant aux utilisateurs ce qui suit :

3.1.1.1.1 Une description de l’application Web;

3.1.1.1.2 Des renseignements sur les étapes à suivre pour obtenir l’accès;

3.1.1.1.3 Un accès aux documents à l’appui;

3.1.1.1.4 Un accès à des points de contact pour obtenir des renseignements supplémentaires ou signaler un problème.

3.1.2 Accéder au journal des risques et des possibilités et y effectuer des recherches

3.1.2.1 Le logiciel de gestion des risques doit afficher uniquement les éléments de risque et de possibilité qu’un utilisateur est autorisé à visualiser et à consulter en fonction de son rôle d’utilisateur.

3.1.2.2 Le logiciel de gestion des risques doit permettre aux utilisateurs de filtrer les recherches qu’ils effectuent dans le journal des risques et des possibilités, au minimum, en fonction des éléments suivants :

3.1.2.2.1 Numéro d’identification unique;

3.1.2.2.2 Élément;

3.1.2.2.3 Type;

3.1.2.2.4 Projet ou programme;

3.1.2.2.5 Classe/flotte;

3.1.2.2.6 Plateformes;

3.1.2.2.7 Système ou équipement;

3.1.2.2.8 Personne responsable (propriétaire);

3.1.2.2.9 Niveau de risque global;

3.1.2.2.10 Statut de l’élément.

3.1.2.3 Le logiciel de gestion des risques doit permettre aux utilisateurs de filtrer les recherches qu’ils effectuent dans le journal des risques et des possibilités en fonction des champs de données clés supplémentaires décrits à la section 3.6.

3.1.2.4 Le logiciel de gestion des risques doit permettre aux utilisateurs de filtrer les recherches qu'ils effectuent dans le journal des risques et des possibilités en fonction des mots clés faisant l'objet de références croisées avec les champs de données décrits à la section 3.6.

3.1.2.5 Le logiciel de gestion des risques doit permettre aux utilisateurs de personnaliser les informations présentées dans le journal des risques et des possibilités (colonnes).

3.1.2.6 Le logiciel de gestion des risques doit permettre aux utilisateurs d'accéder facilement à une liste consolidée des éléments de risque et de possibilité pour lesquels ils sont identifiés comme intervenant clé (p. ex. le propriétaire, l'autorité technique ou l'autorité opérationnelle).

3.1.2.7 Le logiciel de gestion des risques doit permettre aux utilisateurs d'enregistrer des critères de recherche précis ou des filtres pour accéder facilement à des sections spécifiques du journal des risques et des possibilités.

3.1.2.8 Le logiciel de gestion des risques doit permettre aux utilisateurs de télécharger la vue active du journal des risques et des possibilités (en fonction de leurs critères de recherche), au moins dans le format suivant :

3.1.2.8.1 Format PDF;

3.1.2.8.2 Document de type feuille de calcul compatible avec Microsoft Excel.

3.1.3 Rapports

3.1.3.1 Le logiciel de gestion des risques doit permettre aux utilisateurs d'extraire des rapports en fonction de critères et de paramètres de recherche prédéterminés.

3.1.3.2 Le rapport généré doit contenir au moins les renseignements suivants :

3.1.3.2.1 La date et l'heure auxquelles il a été généré;

3.1.3.2.2 Le nom de l'utilisateur qui a généré le rapport;

3.1.3.2.3 Les critères de recherche ayant servi à générer le rapport;

3.1.3.2.4 Les numéros de page.

3.1.3.3 Le logiciel de gestion des risques doit permettre aux utilisateurs de télécharger des rapports au moins dans le format suivant :

3.1.3.3.1 Format PDF.

3.1.3.4 Le logiciel de gestion des risques doit permettre aux utilisateurs de personnaliser l'aspect et la convivialité d'un rapport, y compris les éléments suivants :

3.1.3.4.1 Titre du rapport;

3.1.3.4.2 Désignation et classification de sécurité;

3.1.3.4.3 Avis de non-responsabilité;

3.1.3.4.4 Logo pour la page d'accueil;

3.1.3.4.5 La possibilité d'afficher les risques et les possibilités dans une carte thermique quadrillée qui indique le nombre de risques ou de possibilités ayant reçu leur évaluation du risque globale, et ce, pour chaque case de la carte thermique;

3.1.3.4.6 Les colonnes et les champs à afficher pour les possibilités et les risques inclus dans le rapport.

3.1.3.5 Le logiciel de gestion des risques doit permettre aux utilisateurs de générer un rapport de type nœud papillon pour un élément à risque sélectionné.

3.1.4 Projets et programmes

3.1.4.1 Le logiciel de gestion des risques doit permettre uniquement aux utilisateurs autorisés de créer un nouveau projet ou programme.

3.1.4.2 Le logiciel de gestion des risques doit permettre aux utilisateurs d'accéder facilement à une liste consolidée des éléments de risque et de possibilité liés à un projet ou un programme donné.

3.1.4.3 Le logiciel de gestion des risques doit permettre aux utilisateurs d'accéder facilement à une liste consolidée des projets et des programmes pour lesquels l'utilisateur est considéré comme un intervenant désigné (p. ex. gestionnaire, coordonnateur, administrateur et collaborateur).

3.1.5 Éléments de risque et de possibilité

3.1.5.1 Le logiciel de gestion des risques doit permettre aux utilisateurs d'accéder aux éléments de risque et de possibilité pour lesquels ils ont été autorisés en fonction de leur rôle d'utilisateur.

3.1.5.2 Le logiciel de gestion des risques doit permettre aux utilisateurs de partager et d'accéder aux éléments de risque et de possibilité en fonction d'un lien hypertexte unique.

3.1.5.3 Le logiciel de gestion des risques doit permettre aux utilisateurs de créer des éléments de risque et de possibilité s'ils y sont autorisés en fonction de leur rôle d'utilisateur.

3.1.5.4 Le logiciel de gestion des risques doit permettre aux utilisateurs de créer et de gérer les types d'éléments de risque et de possibilité suivants :

3.1.5.4.1 Éléments de risque et de possibilité par défaut décrits à la section 3.6.3;

3.1.5.4.2 Éléments de risque et de possibilité du projet et du programme décrits à la section 3.6.4;

3.1.5.4.3 Éléments de risque pour la sécurité décrits à la section 3.6.5;

3.1.5.4.4 Éléments de risque liés à la cybersécurité décrits à la section 3.6.6;

3.1.5.4.5 Éléments de risque pour la sécurité des munitions et des explosifs décrits à la section 3.6.7;

3.1.5.4.6 Les éléments de risque liés au matériel naval en service décrits à la section 3.6.8;

3.1.5.4.7 Éléments de risque pour la navigabilité décrits à la section 3.6.9.

3.1.5.5 Le logiciel de gestion des risques doit permettre aux utilisateurs d'accéder à une vue consolidée de tous les éléments qui se rapportent à une évaluation des risques en matière de navigabilité, ce qui comprend :

3.1.5.5.1 L'Évaluation des impacts sur la navigabilité (ÉIN) décrite à la section 3.6.10;

3.1.5.5.2 L'Alerte de risque pour la navigabilité (ARN) décrit à la section 3.6.11;

3.1.5.5.3 L'Alerte de risque sur la navigabilité (ARN) décrite à la section 3.6.12;

3.1.5.5.4 Le Journal de suivi des risques de navigabilité décrit à la section 3.6.13.

3.1.5.6 Le logiciel de gestion des risques doit permettre aux utilisateurs autorisés de configurer des types d'éléments de risque et de possibilité supplémentaires.

3.1.5.7 Le logiciel de gestion des risques doit permettre aux utilisateurs autorisés de modifier les éléments de risque et de possibilité, y compris la modification de leur statut.

3.1.5.8 Le logiciel de gestion des risques doit permettre aux utilisateurs autorisés de supprimer les éléments de risque et de possibilité s'ils n'ont jamais été approuvés.

3.1.5.9 Le logiciel de gestion des risques doit permettre aux utilisateurs autorisés de télécharger un élément de risque ou de possibilité dans le format suivant :

3.1.5.9.1 Format PDF;

3.1.5.9.2 Document de traitement de texte compatible avec Microsoft Word.

3.1.5.10 Le logiciel de gestion des risques doit permettre aux utilisateurs de s'inscrire à un élément de risque ou de possibilité afin de recevoir des avis automatisés personnalisés, notamment :

3.1.5.10.1 Lorsque le statut de l'élément est modifié;

3.1.5.10.2 Lorsque l'élément a été appuyé ou approuvé;

3.1.5.10.3 Lorsqu'un nouveau commentaire est ajouté;

3.1.5.10.4 Lorsque des modifications ont été apportées à l'élément.

3.1.5.11 Le logiciel de gestion des risques doit permettre aux utilisateurs d'ajouter des commentaires aux éléments de risque et de possibilité.

3.1.6 Flux de travaux

3.1.6.1 Le logiciel de gestion des risques doit avoir la capacité d'exécuter des flux de travaux pour l'examen et l'approbation des évaluations de risque et de possibilité, alors qu'une séquence d'événements prédéfinie est réalisée et comprend l'avis automatisé envoyé aux utilisateurs en vue d'effectuer une action ou de recevoir des renseignements.

3.1.6.2 Le logiciel de gestion des risques doit permettre aux utilisateurs autorisés de configurer des flux de travaux pour les éléments de risque et de possibilité.

3.1.6.3 Le logiciel de gestion des risques doit permettre à un utilisateur autorisé de lancer le processus d'examen et d'approbation décrit à la section 9 de l'annexe 6 pour une ARN et pour un RGRN.

3.1.7 Signatures électroniques

3.1.7.1 Le logiciel de gestion des risques doit avoir la capacité de capturer les signatures électroniques en s'appuyant au moins sur l'authentification de l'utilisateur de ce logiciel.

3.1.7.2 Le logiciel de gestion des risques doit inviter l'utilisateur à reconnaître l'intention d'apposer sa signature électronique.

3.1.7.3 Le logiciel de gestion des risques doit indiquer qu'un signataire a examiné ou approuvé l'élément par le biais d'une signature électronique lorsqu'un élément de risque ou de possibilité est téléchargé en format PDF.

3.1.8 Avis automatisés

3.1.8.1 Le logiciel de gestion des risques doit avoir la capacité d'envoyer des avis automatisés, notamment par courriel, pour activer les flux de travaux, pour aviser un utilisateur qui s'est inscrit pour recevoir des avis personnalisés pour un élément de risque ou de possibilité, et pour les événements énumérés aux annexes 4 et 5.

3.1.8.2 Les avis par courriel lancés par le logiciel de gestion des risques doivent pouvoir inclure du texte en anglais et en français.

3.1.8.3 Les avis par courriel doivent utiliser le service de relais du protocole SMTP qui sera fourni par le MDN par l'entremise du hub du PIIND.

3.1.9 Gestion des documents

3.1.9.1 Le logiciel de gestion des risques doit permettre aux utilisateurs autorisés de gérer (téléverser, télécharger, supprimer) les fichiers joints aux éléments de risque et de possibilité.

3.1.9.2 Le logiciel de gestion des risques doit au moins saisir les informations suivantes pour chaque fichier téléversé dans le logiciel de gestion des risques :

3.1.9.2.1 Restriction de l'information, y compris les choix suivants (choix multiples, sélection multiple) :

3.1.9.2.1.1 Marchandises contrôlées;

3.1.9.2.1.2 Propriété intellectuelle;

3.1.9.2.1.3 Renseignements commerciaux confidentiels;

3.1.9.2.2 Sensibilité de l'information, y compris les choix suivants (choix multiples, une seule sélection, champ obligatoire) :

3.1.9.2.2.1 Non sensible;

3.1.9.2.2.2 Protégé A;

3.1.9.2.2.3 Protégé B;

3.1.9.2.3 Titre du fichier (titre par défaut provenant du nom du fichier avant l'extension);

3.1.9.2.4 Type de fichier (type par défaut en fonction de l'extension);

3.1.9.2.5 Fichier téléversé (nom d'utilisateur, généré par le système, provenant de l'utilisateur qui effectue l'action);

3.1.9.2.6 Date de téléversement (date et heure, générée par le système).

3.1.9.3 Le logiciel de gestion des risques doit strictement empêcher tout utilisateur de téléverser, d'accéder, de télécharger ou de supprimer tout fichier joint contenant des restrictions ou un caractère sensible, sauf si l'utilisateur a été autorisé à accéder au niveau de restriction et de sensibilité relatif au fichier.

3.1.10 Identification et accès

3.1.10.1 Le logiciel de gestion des risques doit exploiter les justificatifs d'identité de la plateforme Défense O365 du hub en nuage du PIIND.

3.1.11 Contrôle d'accès en fonction des rôles

3.1.11.1 Le logiciel de gestion des risques doit pouvoir gérer les rôles des utilisateurs afin de restreindre l'accès en lecture et en modification (séparément) aux éléments de risque et de possibilité, ainsi qu'aux pièces jointes, au minimum, en fonction des éléments suivants :

3.1.11.1.1 Élément, décrit à la section 1 de l'annexe 4;

3.1.11.1.2 Type, décrit à la section 1 de l'annexe 4;

3.1.11.1.3 Classe/flotte, décrite à la section 1 de l'annexe 4 et énumérée à l'annexe 2;

3.1.11.1.4 Plateforme, décrite à la section 1 de l'annexe 4 et énumérée à l'annexe 2;

3.1.11.1.5 Restriction et sensibilité des informations, décrites à la section 3.1.9, à la section 1 de l'annexe 4 et à la section 1 de l'annexe 6.

3.1.11.2 Le logiciel de gestion des risques doit permettre de restreindre l'accès en lecture et en modification (séparément) en fonction des rôles décrits à l'annexe 7.

3.1.11.3 Le logiciel de gestion des risques doit permettre aux utilisateurs autorisés d'attribuer des rôles prédéterminés aux utilisateurs afin de contrôler l'accès en lecture et en modification aux éléments de risque et de possibilité.

3.1.12 Surveillance de la sécurité

3.1.12.1 Le logiciel de gestion des risques doit vérifier que les interactions et les événements exécutés par le biais d'une interface avec une application externe (y compris ceux décrits à la section 3.4) proviennent d'applications préautorisées.

3.1.12.2 Le logiciel de gestion des risques doit capturer et envoyer des consignations d'événements au niveau de l'application.

3.1.12.3 Le logiciel de gestion des risques doit capturer et envoyer les consignations d'événements au niveau de l'application énumérées à l'annexe 8.

3.1.12.4 Le logiciel de gestion des risques doit transmettre les consignations d'événements au niveau de l'application à l'application de l'équipe de surveillance de la sécurité de l'informatique en nuage (qui est actuellement Azure Sentinel de Microsoft).

3.2 Exigences relatives au rendement

3.2.1 Chargement

3.2.1.1 Le logiciel de gestion des risques doit pouvoir accueillir un minimum de 500 utilisateurs à la fois.

3.2.1.2 Le logiciel de gestion des risques doit pouvoir accueillir un minimum de 2 000 utilisateurs ayant accès à l'application.

3.2.1.3 Le logiciel de gestion des risques doit utiliser la souplesse du nuage afin d'optimiser ses performances tout en maintenant le coût d'exploitation global à un coût minimum.

3.2.2 Vitesse de transaction

3.2.2.1 Le logiciel de gestion des risques doit pouvoir traiter 95 % des transactions en moins d'une seconde, à l'exception des téléversements et des téléchargements de fichiers, pour un utilisateur situé à Gatineau (Québec) ayant accès à l'application par l'entremise du Réseau étendu de la Défense (RED).

3.2.2.2 Le logiciel de gestion des risques doit pouvoir traiter 99 % des transactions en moins de 10 secondes, à l'exception des téléversements et des téléchargements de fichiers, pour un utilisateur situé à Gatineau (Québec) ayant accès à l'application par l'entremise du RED.

3.3 Exigences relatives à la convivialité

3.3.1 Interface utilisateur sur le Web

3.3.1.1 Le logiciel de gestion des risques doit être accessible par le biais de Google Chrome.

3.3.1.2 Le logiciel de gestion des risques doit être accessible par le biais de Microsoft Edge.

3.3.1.3 L'interface utilisateur du logiciel de gestion des risques doit être conforme à la norme sur l'accessibilité du Web de la réf. [A].

3.3.1.4 L'interface utilisateur du logiciel de gestion des risques doit être conforme aux normes de convivialité du Web de la réf. [B].

3.3.2 Langues officielles

3.3.2.1 L'interface utilisateur du logiciel de gestion des risques doit être disponible en anglais et en français.

3.4 Exigences relatives aux interfaces

3.4.1 Interface avec le réseau en étoile du nuage

3.4.1.1 Le logiciel de gestion des risques doit interagir avec le hub en nuage de l'Active Directory de Microsoft afin de gérer les identifications et les accès.

3.4.2 Interface de programmation d'applications (API)

3.4.2.1 Le logiciel de gestion des risques doit fournir une API afin de permettre l'intégration de futures applications et d'exécuter, au minimum, les fonctions suivantes :

3.4.2.1.1 Créer et modifier des projets et des programmes, y compris tous les champs de données décrits à la section 3.6.1;

3.4.2.1.2 Créer et modifier des éléments de risque et de possibilité, y compris tous les champs de données décrits pour chaque type donné aux sections 3.6.2 à 3.6.9;

3.4.2.1.3 Extraire les données des projets et des programmes, y compris tous les champs de données décrits à la section 3.6.1;

3.4.2.1.4 Extraire les données des éléments de risque et de possibilité, y compris tous les champs de données décrits pour chaque type donné aux sections 3.6.2 à 3.6.9;

3.4.2.1.5 Extraire les données du journal des risques et des possibilités, décrit aux sections 3.1.1.2 à 3.1.1.5;

3.4.2.1.6 Extraire les fichiers PDF générés par le système pour les éléments de risque et de possibilité;

3.4.2.1.7 Extraire les fichiers joints aux éléments de risque et de possibilité.

3.4.2.2 Le logiciel de gestion des risques doit utiliser une norme ouverte pour l'exécution des fonctions API décrites à la section 3.4.3.1.

3.5 Exigences relatives aux bases de données

3.5.1 Toutes les données en transit générées par le logiciel de gestion des risques doivent demeurer entièrement et uniquement sous le contrôle du Canada.

3.5.2 Conformément à l'exigence susmentionnée, toutes les données en transit doivent être stockées dans une installation informatique approuvée par le gouvernement du Canada et située à l'intérieur des frontières géographiques du Canada.[2]

3.5.3 Les réseaux de transit de données doivent être protégés adéquatement grâce à l'utilisation de dispositifs de chiffrement et de mesures de protection des réseaux appropriées.

[2] Les serveurs et les bases de données virtuels, obtenus par le biais d'un contrat de fournisseur de services infonuagiques avec Services partagés Canada, déployés dans une zone de disponibilité au Canada, constituent une solution acceptable.

3.5.4 Le cryptage des données doit être réalisé en utilisant des mécanismes cryptographiques approuvés pour protéger les informations jusqu'au niveau Protégé B, conformément à la réf. [Q].

3.5.5 L'échange de renseignements au moyen de protocoles réseau doit être conforme à la norme de la référence [R].

3.6 Contraintes liées à la conception

3.6.1 Tous les projets et programmes

3.6.1.1 Tous les projets et programmes doivent être conformes aux exigences mentionnées dans l'annexe 5.

3.6.1.2 Par défaut, tous les projets et programmes doivent assigner l'utilisateur qui les a créés comme gestionnaire de projet ou de programme et comme coordinateur de projet ou de programme.

3.6.2 Éléments de risque et de possibilité communs et navals

3.6.2.1 Tous les éléments de risque et de possibilité communs et navals définis dans les sections 3.6.3 à 3.6.8 doivent être conformes aux exigences de la section 1 de l'annexe 4.

3.6.2.2 Par défaut, tous les éléments de risque et de possibilité communs et navals doivent attribuer l'utilisateur qui les a créés comme utilisateur responsable (propriétaire).

3.6.2.3 Tous les éléments de risque et de possibilité communs et navals actifs doivent pouvoir être assortis d'un délai d'expiration au cours duquel ils doivent être revus ou mis à jour, faute de quoi ils deviennent obsolètes. L'objectif est de s'assurer que les propriétaires des éléments revoient régulièrement ceux qui leur sont attribués.

3.6.2.4 Une fois qu'un élément de risque ou de possibilité commun et naval a été accepté ou approuvé, tout changement entraînant un niveau de risque global différent doit annuler l'acceptation ou l'approbation. Le logiciel de gestion des risques doit informer l'utilisateur qui effectue la modification de cette conséquence.

3.6.2.5 Tous les éléments de risque et de possibilité communs et navals doivent permettre le suivi des événements de l'historique suivants :

3.6.2.5.1 date et heure de création de l'élément (date et heure);

3.6.2.5.2 date et heure de la dernière modification de l'état de l'élément (date et heure);

3.6.2.5.3 date et heure de la dernière mise à jour de l'élément (date et heure).

3.6.2.6 Tous les éléments de risque et de possibilité communs et navals doivent inclure les Condition dangereuse, Cause(s) du danger et Effet(s) du danger, de sorte que la relation permettant de soutenir la méthode du nœud papillon décrite dans la norme ISO 31000 puisse être établie[3].

[3] ISO 31000 – Management du risque

3.6.3 Éléments de risque et de possibilité par défaut

3.6.3.1 Tous les éléments de risque et de possibilité par défaut doivent être conformes aux exigences de la section 2 de l'annexe 4.

3.6.4 Éléments de risque et de possibilité des projets et programmes

3.6.4.1 Tous les éléments de risque et de possibilité des projets et programmes doivent être conformes aux exigences de la section 3 de l'annexe 4.

3.6.4.2 Pour tous les éléments de risque et de possibilité des projets et programmes, le champ de projet ou de programme associé décrit dans la section 1 de l'annexe 4 est un champ obligatoire.

3.6.5 Éléments de risque pour la sécurité

3.6.5.1 Tous les éléments de risque pour la sécurité doivent être conformes aux exigences de la section 4 de l'annexe 4.

3.6.6 Éléments de risque liés à la cybersécurité

3.6.6.1 Tous les éléments de risque liés à la cybersécurité doivent être conformes aux exigences de la section 5 de l'annexe 4.

3.6.7 Éléments de risque pour la sécurité des munitions et explosifs

3.6.7.1 Tous les éléments de risque pour la sécurité relatifs aux munitions et explosifs doivent être conformes aux exigences de la section 6 de l'annexe 4.

3.6.8 Éléments de risque liés au matériel naval en service

3.6.8.1 Tous les éléments de risque liés au matériel naval en service doivent être conformes aux exigences de la section 7 de l'annexe 4.

3.6.8.2 Pour tous les risques liés au matériel naval en service, le champ pour Classes / Flotte, Plateformes décrit à la section 1 de l'annexe 4 est un champ obligatoire et ses valeurs doivent être limitées aux classes de la Marine (navires et sous-marins) et aux plateformes de la Marine (navires et sous-marins) énumérées à l'annexe 2.

3.6.8.3 Pour tous les risques liés au matériel naval en service, la sélection du système doit être limitée aux éléments de la référence [K] permettant la sélection du groupe primaire de l'IDDN (champ 2 du code) et de la description de supersystèmes qui lui est associée, conformément à la figure 13-2-1 de la référence [K].

3.6.9 Éléments de risque pour la navigabilité

3.6.9.1 Tous les éléments de risque liés à la navigabilité doivent pouvoir être composés d'au moins un des éléments suivants, mais possiblement de tous :

3.6.9.1.1 l'Évaluation des impacts sur la navigabilité (ÉIN) décrite à la section 3.6.10;

3.6.9.1.2 l'Avis d'alerte de risque (AAR) décrit à la section 3.6.11;

3.6.9.1.3 L'Alerte de risque sur la navigabilité (ARN) décrite à la section 3.6.12;

3.6.9.1.4 le Journal de suivi des risques de navigabilité décrit à la section 3.6.13.

3.6.9.2 Tous les éléments de risque pour la navigabilité doivent pouvoir inclure les éléments suivants :

3.6.9.2.1 le Journal de suivi des risques de navigabilité décrit à la section 3.6.14;

3.6.9.2.2 le Journal d'audit des risques de navigabilité décrit à la section 3.6.15.

3.6.9.3 Tous les composants des éléments de risque liés à la navigabilité énumérés dans la section 3.6.9.1 doivent être conformes aux exigences de la section 1 de l'annexe 6.

3.6.9.4 Tous les composants des éléments de risque liés à la navigabilité énumérés au point 3.6.9.1 doivent pouvoir porter le même numéro de série saisi par l'utilisateur, comme il est décrit au point 1 de l'annexe 6.

3.6.9.5 Tous les composants des éléments de risque liés à la navigabilité énumérés dans la section 3.6.9.1 doivent pouvoir faire l'objet d'un contrôle de version. Plus précisément :

3.6.9.5.1 chaque composant des éléments de risque liés à la navigabilité énumérés dans la section 3.6.9.1 doit pouvoir avoir plusieurs versions accessibles;

3.6.9.5.2 chaque composant des éléments de risque liés navigabilité énuméré dans la section 3.6.9.1 doit uniquement permettre à un utilisateur autorisé de modifier la version actuelle (la plus récente).

3.6.10 Évaluation des impacts sur la navigabilité (ÉIN)

3.6.10.1 Tous les composants de l'évaluation des impacts sur la navigabilité doivent être conformes aux exigences de la section 2 de l'annexe 6.

3.6.10.2 L'évaluation des impacts sur la navigabilité doit pouvoir générer automatiquement un Avis d'alerte de risque à partir de ses données et remplir automatiquement les champs correspondants.

3.6.11 Alerte de risque pour la navigabilité (ARN)

3.6.11.1 Tous les composants de l'alerte de risque pour la navigabilité (ARN) doivent être conformes aux exigences de la section 3 de l'annexe 6.

3.6.11.2 Le logiciel de gestion des risques doit permettre à un utilisateur autorisé d'envoyer l'Avis d'alerte de risque par courriel aux destinataires mentionnés dans la liste de l'Équipe de gestion du risque, dans la liste des intervenants et dans la liste des destinataires.

3.6.11.3 Le courriel de l'Avis d'alerte de risque doit inclure les éléments suivants :

3.6.11.3.1 Les renseignements saisis dans les champs de l'Avis d'alerte de risque décrits à la section 3 de l'annexe 6.

3.6.11.3.2 Un lien hypertexte permettant au destinataire d'accuser réception de l'Avis d'alerte de risque[4].

3.6.11.4 Le courriel de l'Avis d'alerte de risque doit suivre le modèle de la référence [N].

3.6.11.5 Le logiciel de gestion des risques doit permettre d'afficher la date et l'heure auxquelles chaque destinataire d'un Avis d'alerte de risque a accusé réception dudit Avis et d'en faire le suivi.

3.6.11.6 L'Avis d'alerte de risque doit pouvoir générer automatiquement une Alerte de risque sur la navigabilité (ARN) et un Journal de suivi des risques de navigabilité [5]à partir de ses données et remplir automatiquement les champs correspondants.

3.6.12 Alerte de risque sur la navigabilité (ARN)

3.6.12.1 Tous les composants de l'Alerte de risque sur la navigabilité (ARA) doivent être conformes aux exigences de la section 4 de l'annexe 6.

3.6.12.2 Les composants de l'Alerte de risque sur la navigabilité doivent être automatiquement mis au statut « ébauche » au moment de leur création.

3.6.12.3 Les composants de l'Alerte de risque sur la navigabilité doivent être automatiquement mis au statut « approuvé » après avoir reçu toutes les signatures d'approbation.

3.6.12.4 Les composants de l'Alerte de risque sur la navigabilité ne doivent pas être modifiables une fois qu'ils ont été intégrés à un RGRN, fermés, annulés, archivés ou associés à tout autre état signifiant qu'ils ne sont plus actifs.

3.6.12.5 Les composants de l'Alerte de risque sur la navigabilité doivent pouvoir être extraits au format PDF à l'aide du modèle de la référence [O].

3.6.12.6 Les composants de l'Alerte de risque sur la navigabilité doivent pouvoir générer automatiquement un Journal de suivi des risques de navigabilité à partir de l'Alerte de risque sur la navigabilité et remplir automatiquement les champs correspondants.

3.6.13 Journal de suivi des risques de navigabilité

3.6.13.1 Tous les éléments du Journal de suivi des risques de navigabilité doivent être conformes aux exigences de la section 5 de l'annexe 6.

3.6.13.2 Les composants du Journal de suivi des risques de navigabilité doivent pouvoir être extraits au format PDF à l'aide du modèle de la référence [P].

3.6.13.3 Le logiciel de gestion des risques doit empêcher un utilisateur de fermer un Journal de suivi des risques de navigabilité tant que les conditions minimales suivantes n'ont pas été remplies :

3.6.13.3.1 l'indice de risque global se situe au niveau de sécurité acceptable (NSA) pour les risques pour la navigabilité et la survie;

[4] Il est probable que certains destinataires ne disposeront pas d'un compte pour le logiciel de gestion des risques. Ils devraient néanmoins être en mesure d'accuser réception d'une ARN sans avoir besoin d'accéder au logiciel.
[5] L'utilisateur peut choisir de générer l'un ou l'autre, mais il doit avoir la possibilité de générer les deux.

3.6.13.3.2 toutes les activités de contrôle des risques par étapes décrites dans la dernière version du RGRN ont été achevées;

3.6.13.3.3 le propriétaire confirme que le journal de suivi des risques est à jour et indique que (au minimum) toutes les activités de contrôle des risques par étapes sont terminées.

3.6.14 Journal de suivi des risques de navigabilité

3.6.14.1 Tous les composants du Journal de suivi des risques de navigabilité doivent être conformes aux exigences de la section 7 de l'annexe 6.

3.6.14.2 Tous les composants du Journal de suivi des risques de navigabilité doivent permettre aux utilisateurs d'ajouter des événements dans le journal de suivi des risques.

3.6.14.3 Tous les composants du Journal de suivi des risques de navigabilité doivent générer automatiquement des événements du Journal de suivi des risques pour consigner au minimum les éléments suivants :

3.6.14.3.1 le fait qu'une nouvelle version d'un composant de navigabilité (ÉIN, ARN, RGRN) a été approuvée, y compris l'indice de risque global indiqué dans cette version;

3.6.14.3.2 le fait qu'une mesure à prendre du tableau de prévision de l'indice de risque a été effectuée.

3.6.15 Examen de l'audit des risques pour la navigabilité

3.6.15.1 Tous les composants de l'examen de l'audit des risques pour la navigabilité doivent être conformes aux exigences de la section 8 de l'annexe 6.

3.6.15.2 Tous les examens de l'audit des risques pour la navigabilité doivent être associés à une révision précise d'une Évaluation des impacts sur la navigabilité, d'une Alerte de risque sur la navigabilité ou d'un Journal de suivi des risques de navigabilité.

3.6.16 Journaux d'historique

3.6.16.1 Tous les éléments décrits dans la section 3.6 doivent permettre de suivre l'historique des modifications, y compris les données suivantes :

3.6.16.1.1 le membre qui a effectué la modification (nom d'utilisateur);

3.6.16.1.2 la date et l'heure auxquelles la modification a été enregistrée (date et heure);

3.6.16.1.3 l'élément de données qui a été modifié avec sa valeur précédente et sa nouvelle valeur (texte brut).

3.6.16.2 Les journaux d'historique de chaque élément décrit dans la section 3.6 doivent être conservés jusqu'à ce que l'élément en question soit supprimé.

3.7 Attributs du système logiciel

3.7.1 Fiabilité

3.7.1.1 (Laissé intentionnellement vide – voir le point 3.7.3.2 pour l'exigence relative à l'intégrité.)

3.7.2 Disponibilité

3.7.2.1 Comme ce logiciel sera géré par le Canada, les exigences en matière de disponibilité seront déterminées à l'interne.

3.7.3 Sécurité

3.7.3.1 Le logiciel de gestion des risques doit pouvoir traiter et stocker des données jusqu'au niveau Protégé B.

3.7.3.2 Le profil de risque cible pour la solution de gestion des risques doit être Confidentialité des données Protégé B / Intégrité moyenne / Disponibilité moyenne, comme il est décrit dans l'annexe 4A – Profil 1[6] de la référence [E].

3.7.3.3 Le logiciel de gestion des risques et son architecture de soutien doivent être déployés dans des zones de sécurité conformément à la référence [S].

3.7.3.4 Le logiciel de gestion des risques et son architecture de soutien devraient être déployés dans des zones de sécurité en suivant les indications fournies dans la référence [T].

3.7.3.5 Les composants du logiciel-service (le cas échéant) de la solution :

3.7.3.5.1 doivent être conformes à la norme ISO 27 001 Management de la sécurité de l'information[7];

3.7.3.5.2 doivent être conformes à la norme ISO 27 017 Technologies de l'information – Techniques de sécurité – Code de bonnes pratiques pour les contrôles de sécurité de l'information fondés sur l'ISO/IEC 27 002 pour les services du nuage[8];

3.7.3.5.3 doivent être conformes au Service Organization Control (SOC) 2 Type II, tel que détaillé par l'Association of International Certified Professional Accountants (AICPA)[9].

3.7.3.6 La solution logicielle de gestion des risques doit être conforme aux contrôles de sécurité mentionnés dans l'annexe 9.

3.7.3.7 Le logiciel de gestion des risques doit prévoir des mesures préventives pour contrer les 10 principaux risques liés à la sécurité des applications détaillés dans la référence [U].

---

[6] Annexe 4A – Profil 1 – (Protégé B / Intégrité moyenne / Disponibilité moyenne)
https://cyber.gc.ca/fr/orientation/annexe-4a-profil-1-protege-b-integrite-moyenne-disponibilite-moyenne-itsg-33
[7] ISO 27 001 Management de la sécurité de l'information
[8] ISO 27017 — Technologies de l'information — Techniques de sécurité — Services du nuage
[9] SOC 2 Type II de l'AICPA

3.7.4 Maintenabilité

3.7.4.1 Afin de réduire les besoins de maintenance du Canada, la solution doit utiliser des composants de type plateforme-service dans la mesure du possible, à moins que ceux-ci ne soient pas disponibles ou qu'il en soit demandé autrement.

3.7.4.2 Afin de réduire la participation du Programme interarmées d'informatique en nuage de la Défense (PIIND) dans les phases de projet et de mise en service, le nombre de groupes de sécurité du réseau doit être maintenu au minimum nécessaire.

3.7.4.3 Le logiciel de gestion des risques et tous ses composants doivent être déployés sur des serveurs virtuels à l'aide d'images de référence du serveur des systèmes d'information et de communication (SIC).

3.7.4.4 Le logiciel de gestion des risques et tous ses composants doivent être déployés sur des serveurs virtuels à l'aide d'images de référence du serveur SIC de niveau 2, ou d'un niveau supérieur s'il est disponible.

3.7.5 Portabilité

3.7.5.1 Le logiciel de gestion des risques doit permettre la portabilité des données. Plus précisément :

3.7.5.1.1 les données générées par le logiciel de gestion des risques ne doivent pas dépendre de l'utilisation d'une application commerciale propriétaire en particulier;

3.7.5.1.2 les données générées par le logiciel de gestion des risques doivent être la propriété exclusive du gouvernement du Canada.

3.7.5.2 Le logiciel de gestion des risques doit permettre la portabilité des applications. Plus précisément :

3.7.5.2.1 le logiciel de gestion des risques doit être une solution indépendante de la plateforme, ce qui signifie qu'il est portable et interopérable avec les services en nuage d'autres fournisseurs;

3.7.5.2.2 le logiciel de gestion des risques devrait pouvoir être intégré aux processus DevOps et d'intégration continue et de livraison continue (CI/CD) du PIIND à l'aide d'outils en source libre;

3.7.5.2.3 le logiciel de gestion des risques devrait être compatible avec l'utilisation de conteneurs et de serveurs immuables.

3.8 Renseignements connexes

3.8.1 Les éléments suivants sont fournis à l'appui des présentes spécifications des exigences logicielles :

3.8.1.1 Annexe 1 – Sigles

3.8.1.2 Annexe 2 – Liste des plateformes, classes et flottes

3.8.1.3 Annexe 3 – Non utilisée

ANNEXE 1 – SIGLES

SMA(GI)	Sous-ministre adjoint (Gestion de l’information)
API	Interface de programmation d’applications
AC	Armée canadienne
DGGPEA	Directeur général – Gestion du programme d’équipement aérospatial
DGGPEM	Directeur général – Gestion du programme d’équipement maritime
MDN	Ministère de la Défense nationale
SIGRD	Système d’information de gestion des ressources de la défense
RED	Réseau étendu de la Défense
CEI	Commission électrotechnique internationale
ISO	Organisation internationale de normalisation
PIIND	Programme interarmées d’informatique en nuage de la Défense
GCVM	Gestionnaire du cycle de vie du matériel
ENID	Environnement naval intégré des données
ARC	Aviation royale canadienne
MRC	Marine royale du Canada
EDT	Énoncé des travaux
SEL	Spécifications des exigences logicielles
GSTI	Conseils en matière de sécurité des technologies de l’information

ANNEXE 2 – LISTE DES PLATEFORMES, CLASSES ET FLOTTES

MARINE	ARC
Gestionnaires du programme de classe : Grands bâtiments de combat de surface (GBCS) **Classe/flotte** : CLASSE HALIFAX **Plateformes/aéronefs/véhicules** : 330 – NCSM HALIFAX (HAL) 331 – NCSM VANCOUVER (VAN) 332 – NCSM VILLE-DE-QUÉBEC (VDQ) 333 – NCSM TORONTO (TOR) 334 – NCSM REGINA (REG) 335 – NCSM CALGARY (CAL) 336 – NCSM MONTRÉAL (MON) 337 – NCSM FREDERICTON (FRE) 338 – NCSM WINNIPEG (WIN) 339 – NCSM CHARLOTTETOWN (CHA) 340 – NCSM ST-JOHN'S (STJ) 341 – NCSM OTTAWA (OTT) **Gestionnaires du programme de classe** : Grands bâtiments de combat de surface (GBCS) **Classe/flotte** : CLASSE DES NAVIRES DE COMBAT CANADIENS **Plateformes/aéronefs/véhicules** : (À déterminer) **Gestionnaires du programme de classe** : Non affecté au combat (NC) **Classe/flotte** : CLASSE HARRY DEWOLF **Plateformes/aéronefs/véhicules** : 430 – NCSM HARRY DEWOLF (HDW) 431 – NCSM MARGARET BROOKE 432 – NCSM MAX BERNAYS 433 – NCSM WILLIAM HALL 434 – NCSM FRÉDÉRICK ROLETTE 435 – NCSM ROBERT HAMPTON GRAY **Gestionnaires du programme de classe** : Non affecté au combat (NC) **Classe/flotte** : CLASSE PROTECTEUR **Plateformes/aéronefs/véhicules** : 520 – NCSM PROTECTEUR 521 – NCSM PRESERVER **Gestionnaires du programme de classe** : Non affecté au combat (NC) **Classe/flotte** : CLASSE KINGSTON **Plateformes/aéronefs/véhicules** : 700 – NCSM KINGSTON 701 – NCSM GLACE BAY 702 – NCSM NANAIMO 703 – NCSM EDMONTON 704 – NCSM SHAWINIGAN 705 – NCSM WHITEHORSE 706 – NCSM YELLOWKNIFE 707 – NCSM GOOSE BAY 708 – NCSM MONCTON 709 – NCSM SASKATOON	Chasseurs • CF-188 Hornet Aéronefs maritimes • CP-140 Aurora • CH-148 Cyclone Aéronefs de recherche et de sauvetage • CC-115 Buffalo • CC-130H Hercules • CH-149 Cormorant • CC-295 Kingfisher (aéronef de SAR à voilure fixe) Hélicoptères tactiques • CH-146 Griffon • CH-147F Chinook Aéronefs de formation • CT-114 Tutor • CT-155 Hawk • CT-156 Harvard • CT-142 Dash 8 • Planeurs et avions-remorqueurs (Programme de vol à voile des Cadets de l'Air ou PVVCA) Aéronefs de transport • CC-130J Hercules • CC-138 Twin Otter • CC-144 Challenger • CC-150 Polaris • CC-177 Globemaster III Aéronefs inoccupés • CU171 Super Hauler • CU172 Blackjack • CU173 Raven • CU174 Sky Ranger • CU175 Puma • CU176 Skeldar Systèmes divers • Équipement de survie d'aviation (ESA) • Autre

710 – NCSM BRANDON 711 – NCSM SUMMERSIDE **Gestionnaires du programme de classe** : Non affecté au combat (NC) **Classe/flotte** : CLASSE ORCA **Plateformes/aéronefs/véhicules** : PCT 55 – ORCA PCT 56 – RAVEN PCT 57 – CARIBOU PCT 58 – RENARD PCT 59 – WOLF PCT 60 – GRIZZLY PCT 61 – COUGAR PCT 62 – MOOSE **Gestionnaires du programme de classe** : Sous-marins (SM) **Classe/flotte** : CLASSE VICTORIA **Plateformes/aéronefs/véhicules** : 876 – NCSM VICTORIA (VIC) 877 – NCSM WINDSOR (WSR) 878 – NCSM CORNER BROOK (COR) 879 – NCSM CHICOUTIMI (CHI)	

ANNEXE 3 – (NON UTILISÉE)

ANNEXE 4 – LISTE DES ÉLÉMENTS DE RISQUE ET DE POSSIBILITÉ COMMUNS ET NAVALS

1.1. Cette annexe décrit les exigences associées à chaque type de risque et de possibilité.

1.2. « Champ obligatoire » signifie que si le champ ne contient pas une entrée valide, le logiciel de gestion des risques doit avertir l'utilisateur et l'inviter à en fournir une.

Section 1 – Ensemble des risques et des possibilités communs et navals

Partie 1 – Champs

Au minimum, tous les éléments de risque et de possibilité communs et navals doivent comporter les champs suivants :

N°	**Titre**	**Type de champ**	**Exigence**
1.	Risque ou possibilité	Choix multiples, une seule réponse, champ obligatoire	Tous les éléments de risque et de possibilité doivent pouvoir être désignés comme étant soit un risque, soit une possibilité.
2.	Titre	Texte brut, champ obligatoire	Tous les éléments de risque et de possibilité doivent avoir un titre.
3.	Code d'identification	Généré par le logiciel, champ obligatoire	Tous les éléments de risque et de possibilité doivent avoir un code d'identification unique, généré automatiquement par le logiciel.
4.	Numéro d'identification du MDN	Texte brut	Tous les éléments de risque et de possibilité doivent pouvoir être liés à un numéro d'identification généré par un autre système et utilisé au sein du ministère de la Défense nationale comme référence (par exemple : « DN 8406924 »).
5.	Restriction de l'information	Choix multiples, sélection multiple	Tous les éléments de risque et de possibilité doivent permettre de définir des restrictions basées sur la confidentialité de l'information qu'ils contiennent comme suit : a. Contient des renseignements sur les marchandises contrôlées; b. Contient de la propriété intellectuelle; c. Contient de l'information commerciale confidentielle;
6.	Sensibilité de l'information	Choix multiples, une sélection, champ obligatoire	Tous les éléments de risque et de possibilité doivent permettre de définir la sensibilité de l'information comme suit : a. Non sensible; b. Contient de l'information Protégé A; c. Contient de l'information Protégé B.

7.	Élément	Choix multiples, sélection multiple, champ obligatoire	Tous les éléments de risque et de possibilité doivent pouvoir être associés à un élément applicable de la liste suivante : a. Marine royale canadienne (MRC); b. Aviation royale canadienne (ARC); c. Armée canadienne (AC); d. Mauve (MDN).
8.	Type d'élément :	Choix multiples, une seule réponse, champ obligatoire	Le type de tous les éléments de risque et de possibilité doit pouvoir être défini en fonction des valeurs de la liste suivante : a. Risque ou possibilité par défaut; b. Risque ou possibilité de projet et de programme (conformément à la référence [C]); c. Risque pour la sécurité (conformément à la référence [D]); d. Risque lié à la cybersécurité (référence [Sécurité des TI]); e. Risque pour la sécurité des explosifs et des munitions (référence [F]); f. Risque du matériel naval en service (selon les références [H] et [J]); g. Risque pour la navigabilité (selon la référence [L]).
9.	Propriétaire de l'élément	Nom d'utilisateur, champ obligatoire	Tous les éléments de risque et de possibilité doivent avoir un utilisateur responsable (propriétaire).
10.	Projets ou programmes associés	Choix multiples, sélection multiple	Tous les éléments de risque et de possibilité doivent pouvoir être associés à des projets ou à des programmes.
11.	Classes/flottes et plateformes	Choix multiples, sélection multiple	Tous les éléments de risque et de possibilité doivent pouvoir être liés à des classes/flottes (classes de navires ou de sous-marins, flotte d'aéronefs, flotte de véhicules) telles qu'énumérées à l'annexe 2, et à des plateformes (navires, sous-marins, aéronefs, véhicules) telles qu'énumérées à l'annexe 2.
12.	Système	Texte brut (sauf restriction supplémentaire)	Tous les éléments de risque et de possibilité doivent pouvoir être liés à un système.
13.	Code de stockage de système	Texte brut	Tous les éléments de risque et de possibilité doivent pouvoir être liés à un code de stockage de système.
14.	Numéro de série de système	Texte brut	Tous les éléments de risque et de possibilité doivent pouvoir être liés à un numéro de série de système.

15.	Statut	Choix multiples, une seule réponse, champ obligatoire	L'état actuel de tous les éléments de risque et de possibilité doit pouvoir être indiqué afin de permettre de différencier les éléments actifs et inactifs (ou archivés). L'état actuel de tous les éléments de risque et de possibilité doit pouvoir être indiqué afin de permettre de déterminer les différentes étapes du cycle de vie de l'élément, y compris les états « ébauche », « en cours de révision », « approuvé » et « archivé ».
16.	Énoncé de risque	Texte brut	Tous les éléments de risque et de possibilité doivent être accompagnés d'un énoncé de risque ou de possibilité.
17.	Contexte	Texte brut	Tous les éléments de risque et de possibilité doivent permettre d'inclure des renseignements sur le contexte.
18.	Justification de la probabilité	Texte brut	Tous les éléments de risque et de possibilité doivent permettre d'inclure un énoncé de justification pour l'évaluation de la probabilité.
19.	Justification de l'incidence	Texte brut	Tous les éléments de risque et de possibilité doivent permettre d'inclure un énoncé de justification pour l'évaluation de l'incidence.
20.	Mesures d'atténuation	Entrées multiples, texte brut	Tous les éléments de risque et de possibilité doivent permettre d'inclure des mesures d'atténuation.
21.	Niveau de risque global	Généré par le logiciel selon la probabilité et l'incidence du risque	Tous les éléments de risque et de possibilité doivent être associés à un niveau de risque global.
22.	Renseignements supplémentaires	Texte brut	Tous les éléments de risque et de possibilité doivent permettre d'inclure des renseignements supplémentaires.
23.	Pièces jointes	Fichiers multiples	Tous les éléments de risque doivent permettre de joindre plusieurs fichiers, tels que des courriels, des documents PDF et des images, afin de fournir des renseignements supplémentaires et de saisir les acceptations et les approbations.
24.	Mesures à prendre	Mesures à prendre multiples	Tous les éléments de risque et de possibilité doivent permettre d'inclure des mesures à prendre connexes, comme elles sont décrites dans la partie 3 de la section 1 de l'annexe 4.

Partie 2 – Avis automatisés pour tous les éléments de risque et de possibilité

Au minimum, l'avis automatisé suivant doit être envoyé pour tous les éléments de risque et de possibilité :

N°	**Titre**	**Destinataire de l'avis**	**Déclencheur**
1.	Nouveau propriétaire du risque ou de la possibilité	Propriétaire de l'élément de risque ou de possibilité	Un utilisateur a été désigné comme propriétaire d'un élément de risque ou de possibilité

2.	Un risque ou une possibilité doit faire l'objet d'un examen imminent avant son expiration.	Propriétaire de l'élément de risque ou de possibilité	Un élément de risque ou de possibilité expirera au cours de la semaine prochaine.
3.	Un risque ou une possibilité doit faire l'objet d'un examen en raison de son expiration.	Propriétaire de l'élément de risque ou de possibilité	Un élément de risque ou de possibilité a expiré
4.	Un risque ou une possibilité a changé d'état.	Propriétaire de l'élément de risque ou de possibilité	Un élément de risque ou de possibilité a changé d'état (y compris s'il est archivé et supprimé)
5.	Modification d'un risque ou d'une possibilité d'intérêt	L'utilisateur suit le risque ou la possibilité.	Un élément de risque ou de possibilité d'intérêt[10] a été modifié.

Partie 3 – Mesures à prendre

Au minimum, toutes les mesures à prendre doivent comporter les champs suivants :

N°	**Titre**	**Type de champ**	**Exigence**
1.	Code d'identification	Généré par le logiciel, champ obligatoire	Toutes les mesures à prendre doivent être associées un code d'identification unique, généré automatiquement par le logiciel.
2.	Titre	Texte brut, champ obligatoire	Toutes les mesures à prendre doivent pouvoir inclure un titre.
3.	Description	Texte brut	Toutes les mesures à prendre doivent pouvoir inclure une description.
4.	Militaire	Nom d'utilisateur, champ obligatoire	Toutes les mesures à prendre doivent pouvoir être attribuées à un utilisateur.
5.	Date d'échéance	Date, champ obligatoire	Toutes les mesures à prendre doivent pouvoir être associées à une date d'échéance.
6.	Statut	Choix multiples, champ obligatoire	Toutes les mesures à prendre doivent pouvoir être associées à un état parmi les choix suivants : a. Actif b. Terminé

[10] Un élément de risque ou de possibilité est dit « d'intérêt » lorsqu'un utilisateur s'est inscrit pour recevoir des notifications à son sujet.

			c. Annulé

Partie 4 – Avis automatisés pour les mesures à prendre

Au minimum, l'avis automatisé suivant doit être envoyé pour toutes les mesures à prendre :

N°	**Titre**	**Destinataire de l'avis**	**Déclencheur**
1.	Nouveau responsable de la mesure à prendre	Responsable de la mesure à prendre	Un utilisateur a été désigné comme responsable d'une mesure à prendre.
2.	Date d'échéance imminente de la mesure à prendre	Responsable de la mesure à prendre	Une mesure à prendre atteindra sa date d'échéance au cours de la semaine prochaine.
3.	Date d'échéance de la mesure à prendre dépassée	Responsable de la mesure à prendre	Une mesure à prendre a dépassé sa date d'échéance.
4.	Mesures à prendre annulées	Responsable de la mesure à prendre	Une mesure à prendre a été annulée.

Section 2 – Éléments de risque et de possibilité par défaut

Au minimum, les éléments de risque et de possibilité par défaut doivent comporter les champs suivants :

Nº	Titre	Type de champ	Exigence
1.	Probabilité	Choix multiples, une seule réponse	Pour tous les éléments de risque et de possibilité par défaut, la probabilité doit être évaluée sur la base du tableau suivant[11].
2.	Incidence des risques	Choix multiples, une seule réponse	
3.	Incidence de la possibilité	Choix multiples, une seule réponse	
4.	Niveau de risque global	généré par le logiciel	niveau de risque global doit être évalué sur la base de la figure 2 de la référence [C].
5.	Autorité d'acceptation des risques	Nom d'utilisateur	Tous les éléments de risque et de possibilité par défaut doivent permettre de définir l'autorité d'acceptation des risques.
6.	Poste de l'autorité d'acceptation des risques	Texte brut	Tous les éléments de risque et de possibilité par défaut doivent permettre de définir le poste de l'autorité d'acceptation des risques.
7.	Approbation des risques	Date et heure	Tous les éléments de risque et de possibilité par défaut doivent permettre de faire le suivi de la date et de l'heure auxquelles l'élément de risque a été approuvé par l'autorité d'acceptation des risques.

Risk Probability Threshold Criteria

Probability		Definition
Almost Certain (5)	0.61 - 0.99	Expected to occur in most circumstances.
Likely (4)	0.46 - 0.60	Will probably occur in most circumstances.
Possible (3)	0.31 - 0.45	Could occur at some point.
Unlikely (2)	0.16 - 0.30	Not expected to occur.
Rare (1)	0 - 0.15	Occurs in exceptional circumstances only.

[11] Extrait du site intranet Page Web de la gestion des risques liés aux projets du sous-ministre adjoint (Matériels).

Section 3 – Éléments de risque et de possibilité des projets et programmes

Au minimum, les éléments de risque et de possibilité des projets et programmes doivent comporter les champs suivants :

Nº	Titre	Type de champ	Exigence
1.	Phase du projet ou du programme	Choix multiples, réponses multiples	Tous les éléments de risque et de possibilité doivent pouvoir être associés à une des phases des projets ou des programmes : a. Identification; b. Analyse des options; c. Définition; d. Mise en œuvre; e. Clôture; f. En service; g. Élimination.
2.	Probabilité	Choix multiples, une seule réponse	Pour tous les éléments de risque et de possibilité des projets et programmes, la probabilité doit être évaluée sur la base du tableau suivant[12].
3.	Incidence – Risque	Choix multiples, une seule réponse	
4.	Incidence – Possibilité	Choix multiples, une seule réponse	
5.	Niveau de risque global	Généré par le logiciel	et de possibilité des projets et programmes, le niveau de risque global (évaluation) doit être évalué sur la base de la figure 2 de la référence [C].
6.	Évaluation des risques avant atténuation – portée	(évaluation du risque)	Pour tous les éléments de risque et de possibilité des projets et programmes, la probabilité et l'incidence doivent pouvoir être évaluées (avant toute atténuation) pour la catégorie suivante : Portée.
7.	Évaluation des risques avant atténuation – calendrier	(évaluation du risque)	Pour tous les éléments de risque et de possibilité des projets et programmes, la probabilité et l'incidence doivent pouvoir être évaluées (avant toute atténuation) pour la catégorie suivante : Calendrier.
8.	Évaluation des risques avant atténuation – coûts	(évaluation du risque)	Pour tous les éléments de risque et de possibilité des projets et programmes, la probabilité et l'incidence doivent pouvoir être évaluées (avant toute atténuation) pour la catégorie suivante : Coûts.

Risk Probability Threshold Criteria

Probability		Definition
Almost Certain (5)	0.61 - 0.99	Expected to occur in most circumstances.
Likely (4)	0.46 - 0.60	Will probably occur in most circumstances.

Risk Impact Threshold Criteria

Impact	Cost/Budget Objectives	Schedule Objectives	Performance Objectives
Severe (5)	> 15% Cost Increase	>20% Slippage	Failure to meet requirement / lose a major capability
Major (4)	10-15% Cost Increase	10-20% Slippage	Lose a major requirement
Moderate (3)	5-10% Cost Increase	5-10% Slippage	Degradation of a major requirement
Minor (2)	Up to 5% Cost Increase	< 5% Slippage	Experience a reduction in technical performance
Insignificant (1)	Insignificant <$10K Cost Increase	Insignificant Slippage	No significant reduction

[12] Extrait du site intranet Page Web de la gestion des risques liés aux projets du sous-ministre adjoint (Matériels).
[13] Extrait du site intranet Page Web de la gestion des risques liés aux projets du sous-ministre adjoint (Matériels).

9.	Justifications avant atténuation	Texte brut	Tous les éléments de risque et de possibilité des projets et programmes doivent permettre d'inclure un énoncé de justification pour chaque évaluation avant atténuation et pour chaque catégorie.
10.	Niveau de risque global avant atténuation	généré par le logiciel	Tous les éléments de risque et de possibilité des projets et programmes doivent être assortis d'un niveau de risque global avant atténuation basé sur le niveau d'évaluation le plus élevé des trois catégories d'évaluation avant atténuation (portée, calendrier et coûts).
11.	Évaluation des risques après atténuation – portée	(évaluation du risque)	Pour tous les éléments de risque et de possibilité des projets et programmes, la probabilité et l'incidence doivent pouvoir être évaluées (après toute atténuation) pour la catégorie suivante : Portée.
12.	Évaluation des risques après atténuation – calendrier	(évaluation du risque)	Pour tous les éléments de risque et de possibilité des projets et programmes, la probabilité et l'incidence doivent pouvoir être évaluées (après toute atténuation) pour la catégorie suivante : Calendrier.
13.	Évaluation des risques après atténuation – coûts	(évaluation du risque)	Pour tous les éléments de risque et de possibilité des projets et programmes, la probabilité et l'incidence doivent pouvoir être évaluées (après toute atténuation) pour la catégorie suivante : Coûts.
14.	Justifications après atténuation	Texte brut	Tous les éléments de risque et de possibilité des projets et programmes doivent permettre d'inclure un énoncé de justification pour chaque évaluation après atténuation et pour chaque catégorie.
15.	Niveau de risque global	généré par le logiciel	Tous les éléments de risque et de possibilité des projets et programmes doivent être assortis d'un niveau de risque global après atténuation basé sur le niveau d'évaluation le plus élevé des trois catégories d'évaluation après atténuation (portée, calendrier et coûts).
16.	Autorité d'acceptation des risques	Nom d'utilisateur	Tous les éléments de risque et de possibilité des projets et programmes doivent permettre de définir l'autorité d'acceptation des risques.
17.	Poste de l'autorité d'acceptation des risques	Texte brut	Tous les éléments de risque et de possibilité des projets et programmes doivent permettre de définir le poste de l'autorité d'acceptation des risques.
18.	Approbation des risques	Date et heure	Tous les éléments de risque et de possibilité des projets et programmes doivent permettre de faire le suivi de la date et de l'heure auxquelles l'élément de risque a été approuvé par l'autorité d'acceptation des risques.

Section 4 – Éléments de risque pour la sécurité

Au minimum, les éléments de risque pour la sécurité doivent comporter les champs suivants :

N°	Titre	Type de champ	Exigence
1.	Probabilité	Choix multiples, une seule réponse	Pour tous les éléments de risque pour la sécurité, la probabilité doit être évaluée sur la base des niveaux décrits au point 3.26-a de la référence [D].
2.	Incidence	Choix multiples, une seule réponse	Pour tous les éléments de risque pour la sécurité, l'incidence doit être évaluée sur la base des niveaux décrits au point 3.26-b de la référence [D].
3.	Niveau de risque global	généré par le logiciel	Pour tous les éléments de risque pour la sécurité, l'évaluation du risque global doit être calculée sur la base de la matrice des niveaux de risque du point 3.27 de la référence [D].
4.	Évaluation des risques avant atténuation	(évaluation du risque)	Pour tous les éléments de risque pour la sécurité, la probabilité et l'incidence doivent pouvoir être évaluées avant toute atténuation.
5.	Justifications avant atténuation	Texte brut	Tous les éléments de risque pour la sécurité doivent permettre d'inclure un énoncé de justification pour l'évaluation avant toute atténuation.
6.	Évaluation des risques après atténuation	(évaluation du risque)	Pour tous les éléments de risque pour la sécurité, la probabilité et l'incidence doivent pouvoir être évaluées après toute atténuation.
7.	Justifications avant atténuation	Texte brut	Tous les éléments de risque pour la sécurité doivent permettre d'inclure un énoncé de justification pour l'évaluation après toute atténuation.
8.	Autorité d'acceptation des risques	Nom d'utilisateur	Tous les éléments de risque pour la sécurité doivent permettre de définir l'autorité d'acceptation des risques.
9.	Poste de l'autorité d'acceptation des risques	Texte brut	Tous les éléments de risque pour la sécurité doivent permettre de définir le poste de l'autorité d'acceptation des risques.
10.	Approbation des risques	Date et heure	Tous les éléments de risque pour la sécurité doivent permettre de faire le suivi de la date et de l'heure auxquelles l'élément de risque a été approuvé par l'autorité d'acceptation des risques.

Section 5 – Éléments de risque liés à la cybersécurité

Au minimum, les éléments de risque liés à la cybersécurité doivent comporter les champs suivants :

Nº	Titre	Type de champ	Exigence
1.	Système d'information	Texte brut	Tous les éléments de risque liés à la cybersécurité doivent permettre de définir le système d'information connexe qui serait touché.
2.	Probabilité	Choix multiples, une seule réponse	Pour tous les éléments de risque liés à la cybersécurité, la probabilité doit être évaluée sur la base des niveaux décrits au point 3.26-a de la référence [D].
3.	Incidence	Choix multiples, une seule réponse	Pour tous les éléments de risque liés à la cybersécurité, l'incidence doit être évaluée sur la base des niveaux décrits au point 3.26-b de la référence [D].
4.	Niveau de risque global	Généré par le logiciel	Pour toutes les évaluations des catégories d'éléments de risque liés à la cybersécurité, le niveau du risque global (évaluation) doit être calculé sur la base de la matrice des niveaux de risque du point 3.27 de la référence [D].
5.	Évaluation des risques avant atténuation – confidentialité	(évaluation du risque)	Pour tous les éléments de risque liés à la cybersécurité, la probabilité et l'incidence doivent pouvoir être évaluées (avant toute atténuation) pour la catégorie suivante : Confidentialité, comme elle est définie à l'annexe 5 de la référence [E].
6.	Évaluation des risques avant atténuation – intégrité	(évaluation du risque)	Pour tous les éléments de risque liés à la cybersécurité, la probabilité et l'incidence doivent pouvoir être évaluées (avant toute atténuation) pour la catégorie suivante : Intégrité, comme elle est définie à l'annexe 5 de la référence [E].
7.	Évaluation des risques avant atténuation – disponibilité	(évaluation du risque)	Pour tous les éléments de risque liés à la cybersécurité, la probabilité et l'incidence doivent pouvoir être évaluées (avant toute atténuation) pour la catégorie suivante : Disponibilité, comme elle est définie à l'annexe 5 de la référence [E].
8.	Justifications avant atténuation	Texte brut	Tous les éléments de risque liés à la cybersécurité doivent permettre d'inclure un énoncé de justification pour chaque évaluation avant atténuation et pour chaque catégorie (confidentialité, intégrité et disponibilité).
9.	Niveau de risque global avant atténuation	généré par le logiciel	Tous les éléments de risque liés à la cybersécurité doivent être assortis d'un niveau de risque global avant atténuation basé sur le niveau d'évaluation le plus élevé des trois catégories d'évaluation avant atténuation (confidentialité, intégrité et disponibilité).
10.	Évaluation des risques après atténuation – confidentialité	(évaluation du risque)	Pour tous les éléments de risque liés à la cybersécurité, la probabilité et l'incidence doivent pouvoir être évaluées (après toute atténuation) pour la catégorie suivante : Confidentialité.
11.	Évaluation des risques après atténuation – intégrité	(évaluation du risque)	Pour tous les éléments de risque liés à la cybersécurité, la probabilité et l'incidence doivent pouvoir être évaluées (après toute atténuation) pour la catégorie suivante : Intégrité.

12.	Évaluation des risques avant atténuation – disponibilité	(évaluation du risque)	Pour tous les éléments de risque liés à la cybersécurité, la probabilité et l'incidence doivent pouvoir être évaluées (après toute atténuation) pour la catégorie suivante : Disponibilité.
13.	Justifications après atténuation	Texte brut	Tous les éléments de risque liés à la cybersécurité doivent permettre d'inclure un énoncé de justification pour chaque évaluation après atténuation et pour chaque catégorie (confidentialité, intégrité et disponibilité).
14.	Niveau de risque global	généré par le logiciel	Tous les éléments de risque liés à la cybersécurité doivent être assortis d'un niveau de risque global après atténuation basé sur le niveau d'évaluation le plus élevé des trois catégories d'évaluation après atténuation (portée, calendrier et coûts).
15.	Autorité d'acceptation des risques	Nom d'utilisateur	Tous les éléments de risque liés à la cybersécurité doivent permettre de définir l'autorité d'acceptation des risques.
16.	Poste de l'autorité d'acceptation des risques	Texte brut	Tous les éléments de risque liés à la cybersécurité doivent permettre de définir le poste de l'autorité d'acceptation des risques.
17.	Approbation des risques	Date et heure	Tous les éléments de risque liés à la cybersécurité doivent permettre de faire le suivi de la date et de l'heure auxquelles l'élément de risque a été approuvé par l'autorité d'acceptation des risques.

Section 6 – Éléments de risque pour la sécurité des munitions et explosifs

Au minimum, les éléments de risque pour la sécurité des munitions et explosifs doivent comporter les champs suivants :

Nº	Titre	Type de champ	Exigence
1.	Probabilité	Choix multiples, une seule réponse	Pour tous les éléments de risque pour la sécurité des munitions et explosifs, la probabilité doit être évaluée sur la base des niveaux décrits dans le tableau de probabilité des dangers (figure 3-2-2) de la référence [F].
2.	Incidence	Choix multiples, une seule réponse	Pour tous les éléments de risque pour la sécurité des munitions et explosifs, l'incidence (conséquence) doit être évaluée sur la base des niveaux décrits dans le Tableau des conséquences des dangers (figure 3-2-6) de la référence [F].
3.	Niveau de risque global	généré par le logiciel	Pour tous les éléments de risque pour la sécurité des munitions et explosifs, le niveau d'évaluation du risque global (indice) doit être calculé sur la base du tableau d'indice de risque de la figure 3-2-7 de la référence [F].
4.	Évaluation des risques avant atténuation	(évaluation du risque)	Pour tous les éléments de risque pour la sécurité des munitions et explosifs, la probabilité et l'incidence doivent pouvoir être évaluées avant toute atténuation.
5.	Justifications avant atténuation	Texte brut	Tous les éléments de risque pour la sécurité des munitions et explosifs doivent permettre d'inclure un énoncé de justification pour l'évaluation avant atténuation.
6.	Évaluation des risques après atténuation	(évaluation du risque)	Pour tous les éléments de risque pour la sécurité des munitions et explosifs, la probabilité et l'incidence doivent pouvoir être évaluées après toute atténuation.
7.	Justifications avant atténuation	Texte brut	Tous les éléments de risque pour la sécurité des munitions et explosifs doivent permettre d'inclure un énoncé de justification pour l'évaluation après atténuation.
8.	Utilisateur ayant l'autorité pour l'examen technique	Nom d'utilisateur	Tous les éléments de risque pour la sécurité des munitions et explosifs doivent permettre de définir l'autorité responsable de l'examen technique.
9.	Poste de l'utilisateur ayant l'autorité pour l'examen technique	Texte brut	Tous les éléments de risque pour la sécurité des munitions et explosifs doivent permettre de définir le poste de l'autorité responsable de l'examen technique.
10.	Poste de l'utilisateur ayant l'autorité pour l'approbation des risques	Date et heure	Tous les éléments de risque pour la sécurité des munitions et explosifs doivent permettre de faire le suivi de la date et de l'heure auxquelles l'élément de risque a été approuvé par l'autorité responsable de l'examen technique.
11.	Utilisateur ayant l'autorité pour	Nom d'utilisateur	Tous les éléments de risque pour la sécurité des munitions et explosifs doivent permettre de définir l'autorité responsable de l'approbation opérationnelle.

	l'approbation opérationnelle		
12.	Poste de l'utilisateur ayant l'autorité pour l'approbation opérationnelle	Texte brut	Tous les éléments de risque pour la sécurité des munitions et explosifs doivent permettre de définir le poste de l'autorité responsable de l'approbation opérationnelle.
13.	Approbation des risques de l'autorité pour l'approbation opérationnelle	Date et heure	Tous les éléments de risque pour la sécurité des munitions et explosifs doivent permettre de faire le suivi de la date et de l'heure auxquelles l'élément de risque a été approuvé par l'autorité pour l'approbation opérationnelle.

Section 7 – Éléments de risque liés au matériel naval en service

Au minimum, les éléments de risque liés au matériel naval en service doivent comporter les champs suivants :

Nº	Titre	Type de champ	Exigence
1.	Scénario de risque	Choix multiples, une seule réponse, champ obligatoire	Tous les éléments de risque liés au matériel naval en service doivent pouvoir inclure le scénario de risque lié au matériel naval en service qui s'applique parmi les choix suivants, décrits dans la référence [H]. a. Scénario 1 – fondement de la conception et intention de la conception; b. Scénario 2 – base de référence en matière de certification et plan de certification c. Scénario 3 – dérogations à la base de référence en matière de certification d. Scénario 4 – préparation et performance de la mission.
2.	Domaines de sécurité	Choix multiples, réponses multiples	Tous les éléments de risque liés au matériel naval en service doivent pouvoir être associés aux domaines de sécurité figurant au tableau 3-1 de la référence [G].
3.	Dangers	Entrées multiples, texte brut	Tous les éléments de risque liés au matériel naval en service doivent pouvoir inclure la liste des dangers qui pourraient survenir à la suite de la mise en œuvre de la fourniture du matériel.
4.	Probabilité	Choix multiples, une seule réponse	Pour tous les éléments de risque liés au matériel naval en service, la probabilité pour chacune des catégories ci-dessus doit être évaluée sur la base du tableau de la probabilité de l'annexe 1 de la référence [J].
5.	Incidence	Choix multiples, une seule réponse	Pour tous les éléments de risque liés au matériel naval en service, l'incidence (gravité) pour chacune des catégories ci-dessus doit être évaluée sur la base du tableau de la gravité pertinent de l'annexe 1 de la référence [J].
6.	Niveau de risque global	Généré par le logiciel	Pour toutes les évaluations des catégories d'éléments de risque liés au matériel naval en service, le niveau du risque global doit être calculé sur la base de la matrice des niveaux de risque du point 1 de la référence [J].
7.	Évaluation des risques avant atténuation – personnel	(évaluation du risque)	Pour tous les éléments de risque liés au matériel naval en service, la probabilité et l'incidence doivent pouvoir être évaluées (avant toute atténuation) pour la catégorie suivante : Personnel.
8.	Évaluation des risques avant atténuation – matériel	(évaluation du risque)	Pour tous les éléments de risque liés au matériel naval en service, la probabilité et l'incidence doivent pouvoir être évaluées (avant toute atténuation) pour la catégorie suivante : Matériel.
9.	Évaluation des risques avant	(évaluation du risque)	Pour tous les éléments de risque liés au matériel naval en service, la probabilité et l'incidence doivent pouvoir être

	atténuation – mission		évaluées (avant toute atténuation) pour la catégorie suivante : Mission.
10.	Évaluation des risques avant atténuation – environnement	(évaluation du risque)	Pour tous les éléments de risque liés au matériel naval en service, la probabilité et l'incidence doivent pouvoir être évaluées (avant toute atténuation) pour la catégorie suivante : Environnement.
11.	Justifications avant atténuation	Texte brut	Tous les éléments de risque liés au matériel naval en service doivent permettre d'inclure un énoncé de justification pour chaque évaluation avant atténuation et pour chaque catégorie (personnel, matériel, mission et environnement).
12.	Niveau de risque global avant atténuation	généré par le logiciel	Tous les éléments de risque liés au matériel naval en service doivent être assortis d'un niveau de risque global avant atténuation basé sur le niveau d'évaluation le plus élevé des catégories d'évaluation avant atténuation (personnel, matériel, mission et environnement).
13.	Évaluation des risques après atténuation – personnel	(évaluation du risque)	Pour tous les éléments de risque liés au matériel naval en service, la probabilité et l'incidence doivent pouvoir être évaluées (après toute atténuation) pour la catégorie suivante : Personnel.
14.	Évaluation des risques après atténuation – matériel	(évaluation du risque)	Pour tous les éléments de risque liés au matériel naval en service, la probabilité et l'incidence doivent pouvoir être évaluées (après toute atténuation) pour la catégorie suivante : Matériel.
15.	Évaluation des risques après atténuation – mission	(évaluation du risque)	Pour tous les éléments de risque liés au matériel naval en service, la probabilité et l'incidence doivent pouvoir être évaluées (après toute atténuation) pour la catégorie suivante : Mission.
16.	Évaluation des risques après atténuation – environnement	(évaluation du risque)	Pour tous les éléments de risque liés au matériel naval en service, la probabilité et l'incidence doivent pouvoir être évaluées (après toute atténuation) pour la catégorie suivante : Environnement.
17.	Justifications après atténuation	Texte brut	Tous les éléments de risque liés au matériel naval en service doivent permettre d'inclure un énoncé de justification pour chaque évaluation après atténuation et pour chaque catégorie (personnel, matériel, mission et environnement).
18.	Niveau de risque global	généré par le logiciel	Tous les éléments de risque liés au matériel naval en service doivent être assortis d'un niveau de risque global après atténuation basé sur le niveau d'évaluation le plus élevé des catégories d'évaluation après atténuation (personnel, matériel, mission et environnement).
19.	Responsable technique	Nom d'utilisateur	Tous les éléments de risque liés au matériel naval en service doivent permettre de définir le responsable technique.
20.	Poste du responsable technique	Texte brut	Tous les éléments de risque liés au matériel naval en service doivent permettre de définir le poste du responsable technique.

21.	Approbation des risques du responsable technique	Date et heure	Tous les éléments de risque liés au matériel naval en service doivent permettre de faire le suivi de la date et de l'heure auxquelles l'élément de risque a été approuvé par le responsable technique.
22.	Responsable opérationnel	Nom d'utilisateur	Tous les éléments de risque liés au matériel naval en service doivent permettre de définir le responsable opérationnel.
23.	Poste du responsable opérationnel	Texte brut	Tous les éléments de risque liés au matériel naval en service doivent permettre de définir le poste du responsable opérationnel.
24.	Approbation des risques du responsable opérationnel	Date et heure	Tous les éléments de risque liés au matériel naval en service doivent permettre de faire le suivi de la date et de l'heure auxquelles l'élément de risque a été approuvé par le responsable opérationnel.

ANNEXE 5 – PROJETS ET PROGRAMMES

Partie 1 – Champs

Au minimum, les projets et programmes doivent comporter les champs suivants :

Nº	Titre	Type de champ	Exigence
1.	Projet ou programme	Choix multiples, une seule réponse, champ obligatoire	Tous les projets et programmes doivent pouvoir être désignés comme étant soit un projet, soit un programme.
2.	Titre	Texte brut, champ obligatoire	Tous les projets et programmes doivent avoir un titre.
3.	Code d'identification	Généré par le logiciel, champ obligatoire	Tous les projets et programmes doivent avoir un code d'identification unique.
4.	Numéro d'identification du MDN	Texte brut	Tous les projets et programmes doivent pouvoir être liés à un numéro d'identification généré par un autre système et utilisé au sein du ministère de la Défense nationale comme référence (par exemple : « N.002885 »).
5.	Élément	Choix multiples, sélection multiple, champ obligatoire	Tous les projets et programmes doivent pouvoir être associés à un élément applicable de la liste suivante : a. Marine royale canadienne (MRC); b. Aviation royale canadienne (ARC); c. Armée canadienne (AC); d. Mauve (MDN).
6.	Projet ou programme parent	Choix multiples, une seule réponse	Tous les projets et programmes doivent pouvoir être associés à un projet ou programme parent.
7.	Description du projet ou programme	Texte brut	Tous les projets et programmes doivent avoir l'option d'inclure une description.
8.	Gestionnaire du projet ou du programme	Nom d'utilisateur, champ obligatoire	Tous les projets et programmes doivent permettre d'indiquer le gestionnaire du projet ou du programme.
9.	Poste du gestionnaire de projet ou de programme	Texte brut	Tous les projets et programmes doivent permettre d'indiquer le poste du gestionnaire du projet ou du programme.
10.	Coordonnateur de projet ou de programme	Nom d'utilisateur, champ obligatoire	Tous les projets et programmes doivent permettre d'indiquer le coordonnateur du projet ou du programme.
11.	Poste du coordonnateur	Texte brut	Tous les projets et programmes doivent permettre d'indiquer le poste du coordonnateur du projet ou du programme.

	de projet ou de programme		
12.	Administrateurs de projet ou de programme	Nom d'utilisateur (entrées multiples)	Tous les projets et programmes doivent permettre d'indiquer les administrateurs du projet ou du programme.
13.	Poste des administrateurs de projet ou de programme	Texte brut	Tous les projets et programmes doivent permettre d'indiquer le poste des administrateurs du projet ou du programme (pour chaque administrateur).
14.	Collaborateurs du projet ou du programme	Nom d'utilisateur (entrées multiples)	Tous les projets et programmes doivent permettre d'indiquer les collaborateurs du projet ou du programme.
15.	Poste des collaborateurs de projet ou de programme	Texte brut	Tous les projets et programmes doivent permettre d'indiquer le poste des collaborateurs du projet ou du programme (pour chaque collaborateur).

Partie 2 – Avis automatisés pour les projets et programmes

Au minimum, l'avis automatisé suivant doit être envoyé pour toutes les mesures à prendre :

N°	**Titre**	**Destinataire de l'avis**	**Déclencheur**
1.	Nouvel intervenant au projet ou programme	Nouvel intervenant au projet ou programme	Un utilisateur a été désigné comme intervenant à un projet ou à un programme (gestionnaire, coordonnateur, administrateur, collaborateur).
2.	Le projet ou le programme est archivé ou supprimé	Gestionnaire, coordonnateur et administrateurs de projet ou de programme	Un projet ou un programme est archivé ou supprimé

ANNEXE 6 – LISTE DES ÉLÉMENTS DE RISQUE POUR LA NAVIGABILITÉ

Aperçu du processus de navigabilité

Le processus de gestion des risques de la navigabilité est un produit de prise de décisions qui commence par l’identification d’un danger (risque) par tout utilisateur autorisé à utiliser le système. Le processus actuel, défini dans le Processus de gestion des risques pour la navigabilité EMT01.003, sera modifié. Il s’applique toutefois toujours au nouveau système. Il décrit le processus de navigabilité à utiliser au MDN, dans le Programme de navigabilité des Forces armées canadiennes et à la Division - Gestion du programme d’équipement aérospatial.

Pour obtenir des directives sur les normes à suivre, veuillez vous reporter au Manuel de navigabilité technique (MNT) et au Manuel de navigabilité opérationnelle (MNO).

Exigences des politiques et procédures

L’objectif principal du Manuel de navigabilité technique (MNT) est de fournir un niveau de sécurité acceptable (NSA) en réglementant les aspects techniques des activités liées à l’aviation afin de garantir la sûreté des vols et des atterrissages des aéronefs dans toutes les situations.

Les exigences de navigabilité sont également traduites en une instruction détaillée dans le processus opérationnel AF9000, EMT01.003. Il s’agit des politiques permettant d’appliquer les exigences de navigabilité qui sont détaillées dans le document C-05-005-P12/AM-001, Manuel des procédés techniques (MPT) de la Division – Gestion du programme d’équipement aérospatial, Partie 12, dans la Partie 5 du document C-05-005-001/AG-001, Manuel de navigabilité technique (MNT) et dans le chapitre 5 du document B-GA-104-000/FP-001, Manuel de navigabilité opérationnelle (MNO). Cette politique est satisfaite par le Processus AF9000 portant le numéro EMT01.003.

Section 1 – Éléments de risque liés à la navigabilité

Au minimum, les éléments de risque liés à la navigabilité doivent comporter les champs suivants :

Nº	Titre	Type de champ	Exigence
1.	Catégorisation	Choix multiples, une seule réponse, champ obligatoire	Tous les éléments de risque liés à la navigabilité doivent pouvoir être classés dans la catégorie de la navigabilité technique ou de la navigabilité opérationnelle.
2.	Restriction de l'information	Choix multiples, sélection multiple	Tous les éléments de risque liés à la navigabilité doivent permettre de définir des restrictions basées sur la confidentialité de l'information qu'ils contiennent comme suit : a. Contient des renseignements sur les marchandises contrôlées; b. Contient de la propriété intellectuelle; a. Contient de l'information commerciale confidentielle;
3.	Sensibilité de l'information.	Choix multiples, une sélection, champ obligatoire	Tous les éléments de risque liés à la navigabilité doivent permettre de définir la sensibilité de l'information comme suit : a. Non sensible; b. Contient de l'information Protégé A; c. Contient de l'information Protégé B.
4.	Titre	Texte brut, champ obligatoire	Tous les éléments de risque liés à la navigabilité doivent avoir un titre.
5.	Code d'identification unique	Généré par le logiciel, champ obligatoire	Tous les éléments de risques liés à la navigabilité doivent avoir un code d'identification unique.
6.	Numéro de série du dossier	Texte brut	Tous les éléments de risque liés à la navigabilité doivent permettre d'inclure un numéro de série de dossier selon le format prescrit au point 5.4.1 (b) de la référence [M].
7.	Numéro de version	Texte brut	Tous les éléments de risque pour la navigabilité doivent permettre de suivre le numéro de version.
8.	Propriétaire	Nom d'utilisateur, champ obligatoire	Tous les éléments de risque liés à la navigabilité doivent avoir un propriétaire qui en est responsable.
9.	Type d'aéronef	Choix multiples, sélection multiple, champ obligatoire	Tous les éléments de risque liés à la navigabilité doivent indiquer quel type d'aéronef est concerné, sur la base de la liste de l'annexe 2.
10.	Identification du ou des produits	Entrées multiples, Texte brut	Tous les éléments de risque pour la navigabilité doivent pouvoir inclure l'identification du produit.
11.	Résumé de la situation	Texte enrichi	Tous les éléments de risque pour la navigabilité doivent pouvoir inclure un résumé de la situation.
12.	Date de début	Date et heure générées par le logiciel	Une date de début doit être associée à tous les éléments de risque pour la navigabilité.

13.	Date de fin	Date et heure générées par le logiciel	Une date de fin doit être associée à tous les éléments de risque pour la navigabilité.
14.	Équipe de gestion des risques	Entrées multiples, nom d'utilisateur, organisation et rôle	Tous les éléments de risque pour la navigabilité doivent pouvoir contenir la liste des membres de l'équipe de gestion des risques. Chaque membre figurant sur la liste doit pouvoir ajouter le nom d'utilisateur (courriel), l'organisation (en texte brut) et son rôle (en texte brut).
15.	Listes des intervenants	Entrées multiples, nom d'utilisateur, organisation et rôle	Tous les éléments de risque pour la navigabilité doivent pouvoir contenir la liste des intervenants. Chaque membre figurant sur la liste doit pouvoir ajouter le nom d'utilisateur (courriel), l'organisation (en texte brut) et son rôle (en texte brut).

Section 2 – Évaluation des impacts sur la navigabilité (ÉIN)

Au minimum, les divers composants de l'Évaluation des impacts sur la navigabilité doivent comporter les champs suivants :

Nº	Titre	Type de champ	Exigence
1.	Statut	Choix multiples, une sélection, champ obligatoire	Le statut des composants de l'Évaluation des impacts sur la navigabilité doit correspondre à l'un des choix suivants : a. Ébauche b. En cours d'examen c. Approuvé d. Subsumé par un RGRN e. Terminé
2.	Condition dangereuse	Texte brut	Tous les éléments de l'Évaluation des impacts sur la navigabilité doivent pouvoir inclure des conditions dangereuses.
3.	Causes de danger	Entrées multiples	Tous les éléments de l'Évaluation des impacts sur la navigabilité doivent pouvoir inclure des causes de danger.
4.	Effet du danger – Navigabilité	Entrées multiples, évaluation des risques	Tous les éléments de l'Évaluation des impacts sur la navigabilité doivent pouvoir contenir la liste des effets du danger sur la navigabilité. Chaque effet du danger sur la navigabilité dans une alerte de risque sur la navigabilité doit pouvoir comprendre ce qui suit : a. Titre b. Gravité du danger, choix multiples (une sélection) basés sur le tableau A-1 de la référence [M] c. Justification de la gravité du danger (en texte brut) d. Probabilité du danger, choix multiples (une sélection) basés sur le tableau A-3 de la référence [M] e. Justification de la probabilité du danger (en texte brut) Indice de risque pour la navigabilité généré par le logiciel en fonction du tableau A-6 de la référence [M].
5.	Effet du danger – Capacité de survie	Entrées multiples, évaluation des risques	Tous les éléments de l'Évaluation des impacts sur la navigabilité doivent pouvoir contenir la liste des effets du danger sur la capacité de survie. Chaque effet du danger sur la capacité de survie doit pouvoir inclure ce qui suit : a. Titre b. Gravité du danger, choix multiples (une sélection) basés sur le tableau A-4 de la référence [M] c. Justification de la gravité du danger (en texte brut)

			d. Probabilité du danger, choix multiples (une sélection) basés sur le tableau A-5 de la référence [M] e. Justification de la probabilité du danger (en texte brut) Indice de risque pour la capacité de survie généré par le logiciel en fonction du tableau A-6 de la référence [M].
6.	Indice global de risque pour la navigabilité	Généré par le logiciel	Tous les éléments de l'Évaluation des impacts sur la navigabilité doivent inclure l'indice global de risque pour la navigabilité, basé sur l'indice de risque le plus élevé relevé par l'effet du danger sur la navigabilité.
7.	Indice global de risque pour la capacité de survie	Généré par le logiciel	Tous les éléments de l'Évaluation des impacts sur la navigabilité doivent inclure l'indice global de risque pour la capacité de survie, basé sur l'indice de risque le plus élevé relevé par l'effet du danger sur la capacité de survie.
8.	Pièces jointes	Fichiers multiples	Tous les éléments de danger pour la navigabilité doivent permettre de joindre plusieurs fichiers, tels que des courriels, des documents PDF et des images, afin de fournir des renseignements supplémentaires et de saisir les acceptations et les approbations.

Section 3 – Alerte de risque pour la navigabilité (ARN)

Contexte et but : Conformément au point 5.2 de la référence [M], lorsqu'une condition dangereuse réduisant le niveau de sécurité d'un aéronef ou d'une flotte est découverte, il est impératif qu'un Journal de suivi des risques de navigabilité soit préparé et transmis à l'autorité chargée de l'acceptation du risque du commandement opérationnel dans les plus brefs délais. Pour ce faire, il faut produire un Avis d'alerte de risque et une Alerte de risque sur la navigabilité subséquent (qui est une forme simplifiée du RGRN) pour tout problème lié au risque qui n'est pas à un niveau de sécurité acceptable et qui affecte actuellement les aéronefs ou la flotte.

Au minimum, les éléments d'une alerte de risque pour la navigabilité (ARN) doivent comporter les champs suivants :

Nº	Titre	Type de champ	Exigence
1.	Autres destinataires	Entrées multiples, nom d'utilisateur	Tous les éléments d'un Avis d'alerte de risque doivent permettre d'ajouter des destinataires (en plus de ceux qui figurent dans les listes des membres de l'équipe de gestion des risques et des intervenants).
2.	Nature de la condition dangereuse	Texte brut, champ obligatoire	Tous les éléments d'un Avis d'alerte de risque doivent permettre d'indiquer la nature de la condition dangereuse.
3.	Causes de danger	Entrées multiples	Tous les éléments d'un Avis d'alerte de risque doivent permettre d'indiquer les causes de danger.
4.	Effet du danger	Entrées multiples	Tous les éléments d'un Avis d'alerte de risque doivent permettre de préciser les effets du danger.
5.	Type de danger	Choix multiples, une seule réponse	Chaque danger lié à l'Avis d'alerte de risque doit pouvoir se voir octroyer un type de danger, soit pour la navigabilité, soit pour la capacité de survie.
6.	Probabilité de l'effet du danger	Choix multiples, une seule réponse	Chaque effet du danger lié à l'Avis d'alerte de risque doit pouvoir être évalué de sorte à déterminer sa probabilité selon le tableau A-3 de la référence [M] (pour le type « navigabilité ») et selon le tableau A-5 de la référence [M] (pour le type « capacité de survie »).
7.	Gravité de l'effet du danger	Choix multiples, une seule réponse	Chaque effet du danger lié à l'Avis d'alerte de risque doit pouvoir être évalué de sorte à déterminer sa probabilité selon le tableau A-1 de la référence [M] (pour le type « navigabilité ») et selon le tableau A-4 de la référence [M] (pour le type « capacité de survie »).
8.	Évaluation informelle des incidences opérationnelles	Texte brut, champ obligatoire	Tous les éléments d'un Avis d'alerte de risque doivent permettre d'indiquer l'Évaluation des incidences opérationnelles.
9.	Mesures d'atténuation immédiates	Texte brut	Chaque Avis d'alerte de risque doit pouvoir inclure toute mesure d'atténuation immédiate dont la mise en œuvre est suggérée.
10.	Diffusion d'un ARN ou du RGRN	Date et heure	Les Avis d'alerte de risque doivent indiquer quand l'ARN ou le RGRN est censé être distribué.

11.	Avis de non-responsabilité	Texte brut	Tous les avis d'alerte de risque doivent pouvoir comprendre un avis de non-responsabilité. Voici l'avis de non-responsabilité à utiliser par défaut : *« Les renseignements contenus dans cet avis d'alerte de risque sont préliminaires et peuvent être inexacts. Le contenu peut être révisé dans l'alerte de risque sur la navigabilité ou le Journal de suivi des risques de navigabilité*. »
12.	Date de diffusion	Date et heure (champ généré par le système)	Tous les avis d'alerte de risque doivent permettre de suivre la date et l'heure de diffusion (l'envoi) de l'Avis d'alerte de risque aux destinataires.
13.	Accusé de réception des bénéficiaires	Date et heure (champ généré par le système)	Tous les avis d'alerte de risque doivent pouvoir suivre l'accusé de réception de chaque destinataire.

Section 4 – Alerte de risque sur la navigabilité (ARN)

Contexte et but : Conformément au point 5.3 de la référence [M], l'objectif d'un ARN est d'informer les intervenants : a) de la situation et du niveau de risque estimé; b) des mesures prises pour déterminer pleinement le niveau de risque réel; c) de toute activité de contrôle des risques prévue ou mise en place comme mesure provisoire. En outre, conformément à la référence [O], l'objectif est d'informer l'autorité chargée de l'acceptation du commandement opérationnel de toute nouvelle situation (ou de tout changement important dans une situation existante) mettant en péril la navigabilité aérienne de l'ensemble ou d'une partie des aéronefs d'une flotte donnée et de faire accepter le risque connexe.

Au minimum, les éléments d'une alerte de risque pour la navigabilité doivent comporter les champs suivants :

Nº	Titre	Type de champ	Exigence
	SOUS-SECTION CONCERNANT L'INDICATION DES ÉLÉMENTS DE RISQUE GÉNÉRAUX		
1.	Statut	Choix multiples, une sélection, champ obligatoire	Le statut des éléments d'une alerte de risque pour la navigabilité doit correspondre à l'un des choix suivants : a. Ébauche b. En cours d'examen c. Approuvé d. Subsumé par un RGRN e. Terminé f. Annulé
	SOUS-SECTION CONCERNANT L'INDICATION DES DANGERS		
2.	Condition dangereuse	Texte brut	Tous les éléments d'alerte de risque pour la navigabilité doivent pouvoir comprendre des conditions dangereuses.
3.	Causes de danger	Entrées multiples	Tous les éléments d'alerte de risque pour la navigabilité doivent pouvoir comprendre les causes de danger.
	SOUS-SECTION CONCERNANT L'ÉVALUATION DES RISQUES		
4.	Effet du danger – Navigabilité	Entrées multiples, évaluation des risques	Tous les éléments d'alerte de risque pour la navigabilité doivent pouvoir contenir la liste des effets du danger sur la navigabilité. Chaque effet du danger sur la navigabilité dans une alerte de risque sur la navigabilité doit pouvoir comprendre ce qui suit : a. Titre b. Gravité du danger, choix multiples (une sélection) basés sur le tableau A-1 de la référence [M] c. Justification de la gravité du danger (en texte brut) d. Probabilité du danger, choix multiples (une sélection) basés sur le tableau A-3 de la référence [M] e. Justification de la probabilité du danger (en texte brut) f. Indice de risque pour la navigabilité généré par le logiciel en fonction du tableau A-6 de la référence [M].
5.	Effet du danger – Capacité de survie	Entrées multiples, évaluation des risques	Tous les éléments d'alerte de risque pour la navigabilité doivent pouvoir contenir la liste des effets du danger sur la capacité de survie.

			Chaque effet du danger sur la capacité de survie doit pouvoir inclure ce qui suit : a. Titre b. Gravité du danger, choix multiples (une sélection) basés sur le tableau A-4 de la référence [M] c. Justification de la gravité du danger (en texte brut) d. Probabilité du danger, choix multiples (une sélection) basés sur le tableau A-5 de la référence [M] e. Justification de la probabilité du danger (en texte brut) f. Indice de risque pour la capacité de survie généré par le logiciel en fonction du tableau A-6 de la référence [M].
6.	Indice de risque pour la navigabilité	Généré par le logiciel	Tous les éléments d'alerte de risque pour la navigabilité doivent inclure l'indice global de risque pour la navigabilité, basé sur l'indice de risque le plus élevé relevé par l'effet du danger sur la navigabilité.
7.	Indice de risque pour la capacité de survie	Généré par le logiciel	Tous les éléments d'alerte de risque pour la navigabilité doivent comprendre l'indice global de risque pour la capacité de survie, basé sur l'indice de risque le plus élevé relevé par l'effet du danger sur la capacité de survie.
8.	Niveau de confiance	Texte brut	Tous les éléments d'alerte de risque pour la navigabilité doivent pouvoir comprendre le niveau de confiance.
	SOUS SECTION CONCERNANT LE PLAN D'ATTÉNUATION IMMÉDIATE DES RISQUES		
9.	Prochaines révisions	Texte brut	Tous les éléments d'alerte de risque pour la navigabilité doivent pouvoir comprendre un plan pour les prochaines révisions.
10.	Plan d'atténuation immédiate	Texte brut	Tous les éléments d'alerte de risque pour la navigabilité doivent pouvoir inclure toute mesure immédiate d'atténuation des risques dont la mise en œuvre est suggérée.
11.	Activités immédiates de contrôle des risques	Entrées multiples, texte brut	Tous les éléments d'alerte de risque pour la navigabilité doivent pouvoir inclure des activités immédiates de contrôle des risques, comme le décrit le point 5.3.1 de la référence [M].
12.	Restrictions ou limitations de vol assujetties à l'acceptation du risque du commandement opérationnel	Entrées multiples, texte brut	Tous les éléments d'alerte de risque pour la navigabilité doivent pouvoir inclure toute restriction ou limitation de vol assujettie à l'acceptation du risque du commandement opérationnel.
	SOUS-SECTION CONCERNANT LES PIÈCES JOINTES		
13.	Pièces jointes	Fichiers multiples	Tous les éléments d'alerte de risque pour la navigabilité doivent permettre de joindre plusieurs fichiers, tels que des

			courriels, des documents PDF et des images, afin de fournir des renseignements supplémentaires et de saisir les acceptations et les approbations.
	SOUS-SECTION CONCERNANT L'APPROBATION L'ACCEPTATION DES RISQUES		
14.	Approbation de l'autorité de navigabilité technique	Signature d'approbation	Tous les éléments d'alerte de risque pour la navigabilité doivent permettre le suivi de l'approbation de l'autorité de navigabilité technique. La signature d'approbation doit comprendre ce qui suit : a. Nom d'utilisateur (courriel) b. Nom complet (en texte brut) c. Rang (en texte brut) d. Poste (en texte brut) e. Numéro de téléphone (en texte brut) f. Décision (choix multiples, une seule réponse : « Approuvé » ou « Non approuvé ») g. Justification de la décision (en texte brut) h. Horodatage de la décision (date et heure)
15.	Approbation de l'examen par le personnel de l'autorité indépendante de navigabilité technique	Signature d'approbation	Tous les éléments d'alerte de risque pour la navigabilité doivent permettre le suivi de l'approbation de l'examen par le personnel de l'autorité indépendante de navigabilité technique pour l'indice global de risque élevé et extrêmement élevé. La signature d'approbation doit comprendre ce qui suit : a. Nom d'utilisateur (courriel) b. Nom complet (en texte brut) c. Rang (en texte brut) d. Poste (en texte brut) e. Numéro de téléphone (en texte brut) f. Décision (choix multiples, une seule réponse : « Approuvé » ou « Non approuvé ») g. Justification de la décision (en texte brut) h. Horodatage de la décision (date et heure)
16.	Approbation de l'autorité de navigabilité opérationnelle	Signature d'approbation	Tous les éléments d'alerte de risque pour la navigabilité doivent permettre le suivi de l'approbation de l'autorité de navigabilité opérationnelle. La signature d'approbation doit comprendre ce qui suit : a. Nom d'utilisateur (courriel) b. Nom complet (en texte brut) c. Rang (en texte brut) d. Poste (en texte brut) e. Numéro de téléphone (en texte brut) f. Décision (choix multiples, une seule réponse : « Approuvé » ou « Non approuvé ») g. Justification de la décision (en texte brut) h. Horodatage de la décision (date et heure)

17.	Acceptation du risque du commandement opérationnel	Signature d'approbation	Tous les éléments d'alerte de risque pour la navigabilité doivent permettre le suivi de l'approbation de l'autorité opérationnelle. La signature d'approbation doit comprendre ce qui suit : a. Nom d'utilisateur (courriel) b. Nom complet (en texte brut) c. Rang (en texte brut) d. Poste (en texte brut) e. Numéro de téléphone (en texte brut) f. Décision (choix multiples, une seule réponse : « Approuvé » ou « Non approuvé ») g. Justification de la décision (en texte brut) h. Horodatage de la décision (date et heure)
	SOUS-SECTION CONCERNANT LES COMMENTAIRES		
18.	Commentaires	Entrées multiples, texte brut	Tous les éléments d'alerte de risque pour la navigabilité doivent permettre de recueillir les commentaires des utilisateurs. Chaque commentaire ajouté à un élément d'alerte de risque pour la navigabilité doit comporter ce qui suit : a. Nom d'utilisateur (courriel) de l'auteur b. Commentaire (en texte brut) c. Horodatage de la publication du commentaire (date et heure)

Étape 5 – Journal de suivi des risques de navigabilité

Au minimum, les éléments du Journal de suivi des risques de navigabilité doivent comporter les champs suivants :

Nº	Titre	Type de champ	Exigence
	SOUS-SECTION CONCERNANT L'INDICATION DES ÉLÉMENTS DE RISQUE GÉNÉRAUX		
1.	Statut	Choix multiples, une sélection, champ obligatoire	Le statut des éléments du Journal de suivi des risques de navigabilité doit correspondre à l'un des choix suivants (référence [M], point 5.10) : a. Ébauche b. Ouvert-actif c. Ouvert-inactif d. Ouvert-en révision e. Terminé f. Annulé
	SOUS-SECTION CONCERNANT L'INDICATION DES DANGERS		
2.	(identique à l'ARN)	(identique à l'ARN)	(identique à l'ARN)
	SOUS-SECTION CONCERNANT L'ÉVALUATION DES RISQUES		
3.	(identique à l'ARN)	(identique à l'ARN)	(identique à l'ARN)
	SOUS-SECTION POUR LE PLAN DE CONTRÔLE DES RISQUES		
4.	Options du contrôle des risques	Entrées multiples, texte brut	Tous les éléments du Journal de suivi des risques de navigabilité doivent permettre l'indication des options de contrôle des risques.
5.	Analyse des options	Texte enrichi	Tous les éléments du Journal de suivi des risques de navigabilité doivent pouvoir inclure une analyse des options.
6.	Option préconisée	Texte brut	Tous les éléments du Journal de suivi des risques de navigabilité doivent permettre l'indication d'une option préconisée.
7.	Mise en œuvre du plan	Texte enrichi	Tous les éléments du Journal de suivi des risques de navigabilité doivent pouvoir inclure une description de la mise en œuvre du plan.
8.	Tableau de prévision de l'indice de risque	(Tableau de prévision de l'indice de risque)	Tous les éléments du Journal de suivi des risques de navigabilité doivent pouvoir inclure un tableau de prévision de l'indice de risque comme le décrit la section 6 de l'annexe 6, pour le suivi des mesures à prendre.
	SOUS-SECTION CONCERNANT LES PIÈCES JOINTES		
9.	(identique à l'ARN)	(identique à l'ARN)	(identique à l'ARN)
	SOUS-SECTION CONCERNANT L'APPROBATION L'ACCEPTATION DES RISQUES		
10.	(identique à l'ARN)	(identique à l'ARN)	(identique à l'ARN)
	SOUS-SECTION CONCERNANT LES COMMENTAIRES		
11.	(identique à l'ARN)	(identique à l'ARN)	(identique à l'ARN)

Section 6 – Tableau de prévision de l'indice de risque

Au minimum, le Tableau de prévision de l'indice de risque doit comprendre le champ suivant :

Nº	Titre	Type de champ	Exigence
1.	Code d'identification unique	Généré par le logiciel, champ obligatoire	Toutes les mesures de contrôle des risques doivent avoir un code d'identification unique.
2.	Titre de la mesure de contrôle des risques	Texte brut, champ obligatoire	Toutes les mesures de contrôle des risques doivent avoir un titre.
3.	Description de la mesure de contrôle des risques	Texte enrichi	Toutes les mesures de contrôle des risques doivent pouvoir inclure une description.
4.	Importance	Choix multiples, une sélection	Toutes les mesures de contrôle des risques doivent permettre l'ajout d'un niveau d'importance : a. Étape b. Autre
5.	Étape	Choix multiples, une sélection	Toutes les mesures de contrôle des risques doivent pouvoir être indiquées comme une étape (choix de réponse « oui » ou « non »).
6.	Date de fin prévue	Date	Toutes les mesures de contrôle des risques doivent permettre l'ajout d'une date de fin prévue pour chaque mesure.
7.	Organisation affectée	Texte brut	Toutes les mesures de contrôle des risques doivent permettre l'affectation d'une organisation.
8.	Utilisateur affecté	Nom d'utilisateur	Toutes les mesures de contrôle des risques doivent permettre l'affectation d'un utilisateur.
9.	Indice de risque résiduel	Choix multiples, une sélection	Toutes les mesures de contrôle des risques doivent permettre l'indication d'un indice de risque résiduel en fonction des choix d'indice de risque figurant à la référence [M].
10.	Justification de l'indice de risque résiduel	Texte brut	Toutes les mesures de contrôle des risques doivent pouvoir inclure une justification de l'indice de risque résiduel.
11.	Statut	Généré par le logiciel, champ obligatoire	Toutes les mesures de contrôle des risques doivent se voir attribuer un des statuts suivants : a. Actif b. Terminé (attribué lorsqu'une date de fin est saisie) c. En retard (attribué si l'élément n'est pas terminé après la date d'échéance) d. Date d'échéance revue (statut attribuable seulement aux éléments qui ne sont pas des étapes)
12.	Date de fin réelle	Date	Toutes les mesures de contrôle des risques doivent permettre l'ajout d'une date de fin.
13.	Renseignements supplémentaires	Texte enrichi	Toutes les mesures de contrôle des risques doivent permettre l'ajout de renseignements.

Section 7 – Journal de suivi des risques

Au minimum, le Journal de suivi des risques de navigabilité doit comporter le champ suivant :

Nº	Titre	Type de champ	Exigence
1.	Code d'identification unique	Généré par le logiciel, champ obligatoire	Tous les éléments du Journal de suivi des risques de navigabilité doivent avoir un code d'identification unique.
2.	Définition des risques connexes pour la navigabilité	Texte brut, généré par le logiciel	Tous les éléments du Journal de suivi des risques de navigabilité doivent être associés à un risque pour la navigabilité.
3.	Élément connexe du Tableau de prévision de l'indice de risque	(Élément connexe du Tableau de prévision de l'indice de risque)	Tous les éléments du Journal de suivi des risques de navigabilité doivent pouvoir être liés à un élément existant du Tableau de prévision de l'indice de risque. Le statut des éléments corrélés du Tableau de prévision de l'indice de risque sera modifié conformément au point 11 de la section 6.
4.	Tableau du Journal de suivi des risques de navigabilité	Entrées multiples, événements du Journal de suivi des risques de vérification	Tous les éléments du Journal de suivi des risques de navigabilité doivent pouvoir inclure des événements du Journal de suivi des risques, comme le décrit la partie 2 de la section 7 de l'annexe 6.

Partie 2 – Événement du Journal de suivi des risques

Nº	Titre	Type de champ	Exigence
1.	Code d'identification unique	Généré par le logiciel, champ obligatoire	Tous les événements du Journal de contrôle des risques doivent avoir un code d'identification unique.
2.	Titre	Texte brut, champ obligatoire	Tous les événements du Journal de contrôle des risques doivent avoir un titre.
3.	Description	Texte brut	Tous les événements du Journal de contrôle des risques doivent pouvoir inclure une description.
4.	Date	Date, champ obligatoire	Tous les événements du Journal de contrôle des risques doivent indiquer la date de la consignation de l'événement.
5.	Nom d'utilisateur	Nom d'utilisateur	Un utilisateur doit être associé à tous les événements du Journal de contrôle des risques.

Section 8 – Examen de la vérification des risques pour la navigabilité

Au minimum, l'examen de vérification des risques pour la navigabilité doit comporter le champ suivant :

N°	Titre	Type de champ	Exigence
1.	Code d'identification unique	Généré par le logiciel, champ obligatoire	Tous les éléments de l'examen de la vérification des risques pour la navigabilité doivent avoir un code d'identification unique.
2.	Composante connexe au risque pour la navigabilité	Texte brut, généré par le logiciel	Tous les éléments de l'examen de la vérification des risques pour la navigabilité doivent être associés à une version précise d'une Évaluation des impacts sur la navigabilité, d'une alerte au risque de navigabilité ou d'un Journal de suivi des risques de navigabilité.
3.	Date	Date, généré par le logiciel	Tous les éléments de l'examen de la vérification des risques pour la navigabilité doivent indiquer la date à laquelle a eu lieu l'examen de la vérification.
4.	Tableau des lacunes de l'examen de la vérification	Entrées multiples, lacunes de l'examen de la vérification	Tous les éléments de l'examen de la vérification des risques pour la navigabilité doivent pouvoir inclure une liste des lacunes, comme le décrit la partie 2 de la section 8 de l'annexe 6.
5.	Renseignements supplémentaires	Texte enrichi	Tous les éléments de l'examen de la vérification des risques pour la navigabilité doivent permettre l'ajout de renseignements.

Partie 2 – Lacunes de l'examen de la vérification

N°	Titre	Type de champ	Exigence
1.	Code d'identification unique	Généré par le logiciel, champ obligatoire	Toutes les lacunes de la vérification doivent avoir un code d'identification unique.
2.	Titre	Texte brut, champ obligatoire	Toutes les lacunes de la vérification doivent avoir un titre.
3.	Description	Texte enrichi	Toutes les lacunes de la vérification doivent pouvoir inclure une description.
4.	Importance	Choix multiples, une sélection	Toutes les lacunes de la vérification doivent permettre l'ajout d'un niveau d'importance : a. Normal b. Important c. Essentiel

Section 9 – Processus d'examen et d'approbation de la navigabilité

1. Voici le processus d'examen et d'approbation des éléments de navigabilité (ARN et RGRN) :

Étape	Type	Mesure
1.	Entrée de l'utilisateur	Un utilisateur autorisé lance le processus d'examen et d'approbation.
2.	Logiciel	L'autorité de navigabilité technique est informée que son action est requise.
3.	Entrée de l'utilisateur	L'autorité de navigabilité technique saisit sa décision et sa signature électronique.
4.	Logiciel	Si l'indice global de risque est élevé ou extrêmement élevé, le personnel de l'autorité indépendante de navigabilité technique chargé de l'examen est informé que son action est requise.
5.	Entrée de l'utilisateur	Si l'indice global de risque est élevé ou extrêmement élevé, l'autorité indépendante de navigabilité technique saisit sa décision et sa signature électronique.
6.	Logiciel	L'autorité de navigabilité opérationnelle est informée que son action est requise.
7.	Entrée de l'utilisateur	L'autorité de navigabilité opérationnelle saisit sa décision et sa signature électronique.
8.	Logiciel	Le commandement opérationnel est informé que son action est requise.
9.	Entrée de l'utilisateur	Le commandement opérationnel saisit sa décision et sa signature électronique.
10.	Logiciel	Les intervenants (c'est-à-dire l'équipe de gestion des risques et les personnes figurant sur la liste des intervenants) sont informés de la fin du processus.
11.	Logiciel	La version actuelle est verrouillée si elle est entièrement approuvée. Le propriétaire du risque peut créer une nouvelle version s'il y a lieu.

2. Si l'une des autorités de révision ou d'approbation sélectionne pendant le processus « non approuvé », le propriétaire en est informé, et le processus est interrompu.

ANNEXE 7 – CONTRÔLE DES ACCÈS EN FONCTION DES RÔLES

Cette annexe contient des propositions de rôles par défaut à activer dans le logiciel de gestion des risques pour que soit séparé le niveau d'accès selon les besoins des utilisateurs. Conformément au point 3.1.11, chaque utilisateur doit pouvoir être restreint quant aux aspects particuliers, comme la classe ou la flotte.

Section 1 – Rôles d'administrateur

RÔLE	LIRE	MODIFIER
Administrateur du système	Tous	Tous
Administrateur de la Marine	Tous, Marine et mauve seulement	Tous, Marine et mauve seulement
Administrateur de la Force aérienne	Tous, Force aérienne et mauve seulement	Tous, Force aérienne et mauve seulement
Administrateur mauve	Tous, mauve seulement	Tous, mauve seulement

Section 2 – Rôles mauve

RÔLE	LIRE	MODIFIER
Utilisateur mauve	Peut lire tous les éléments (mauve seulement)	Peut créer de nouveaux éléments (mauve seulement) Peut créer un nouveau projet ou programme (mauve seulement) Peut modifier les éléments dont il est le propriétaire ou un approbateur (mauve seulement)
Mauve seulement	Peut lire tous les éléments qui n'ont aucune restriction d'information (mauve seulement), à l'exception des éléments qui lui sont attribués en tant que propriétaire	Peut créer de nouveaux éléments (mauve seulement) Peut modifier les éléments dont il est le propriétaire ou un approbateur (mauve seulement)

Section 3 – Rôles de la Marine

RÔLE	LIRE	MODIFIER
Utilisateur de la Marine	Peut lire tous les éléments (Marine et mauve seulement)	Peut créer de nouveaux éléments (marine et mauve seulement) Peut créer un nouveau projet ou programme (Marine et mauve seulement) Peut modifier les éléments dont il est le propriétaire ou un approbateur (mauve seulement)
Marine seulement	Peut lire tous les éléments qui n'ont aucune restriction d'information (Marine et mauve seulement), à l'exception des éléments qui lui sont attribués en tant que propriétaire	Peut créer de nouveaux éléments (marine et mauve seulement) Peut modifier les éléments dont il est le propriétaire ou un approbateur (Marine et mauve seulement)

Section 4 – Rôles de la Force aérienne

RÔLE	LIRE	MODIFIER
Utilisateur de la Force aérienne	Peut lire tous les éléments (Force aérienne et mauve seulement)	Peut créer de nouveaux éléments (Force aérienne et mauve seulement) Peut créer un nouveau projet ou programme (Force aérienne et mauve seulement)

		Peut modifier les éléments dont il est le propriétaire ou un approbateur (mauve seulement)
Force aérienne seulement	Peut lire tous les éléments qui n'ont aucune restriction d'information (Force aérienne et mauve seulement), à l'exception des éléments qui lui sont attribués en tant que propriétaire	Peut créer de nouveaux éléments (Force aérienne et mauve seulement) Peut modifier les éléments dont il est le propriétaire ou un approbateur (Force aérienne et mauve seulement)

Section 5 – Rôles des projets et des programmes

	Rôle du système	Rôle des intervenants du projet ou du programme			
	Administrateur	Gestionnaire	Coordonnateur	Administrateurs	Collaborateurs
Lire les éléments sous le projet ou le programme	X	X	X	X	X
Créer de nouveaux éléments sous le projet ou le programme	X	X	X	X	X
Modifier tout élément associé au projet ou au programme	X	X	X	X	
Ajouter et supprimer des utilisateurs « Collaborateurs »	X	X	X	X	
Ajouter et supprimer des utilisateurs « Administrateurs »	X	X	X	X	
Modifier l'utilisateur « Coordinateur »	X	X	X		
Modifier l'utilisateur « Gestionnaire »	X	X			

ANNEXE 8 – LISTE DES JOURNAUX D'APPLICATIONS

Voici une liste des journaux d'applications recommandés :

Authentification [AUTHN]
authn_login_success[:userid]
authn_login_successafterfail[:userid,retries]
authn_login_fail[:userid]
authn_login_fail_max[:userid,maxlimit(int)]
authn_login_lock[:userid,reason]
authn_token_delete[:appid]
authn_password_change[:userid]
authn_impossible_travel[:userid,region1,region2]
authn_token_created[:userid, entitlement(s)]
authn_token_revoked[:userid,tokenid]
authn_token_reuse[:userid,tokenid]

Autorisation [AUTHZ]
authz_fail[:userid,resource]
authz_change[:userid,from,to]
authz_admin[:userid,event]

Utilisation excessive [EXCESS]
excess_rate_limit_exceeded[userid,max]

Téléversement de fichiers [UPLOAD]
upload_complete[userid,filename,type]
upload_stored[filename,from,to]
upload_validation[filename,(virusscan|imagemagick|...):(FAILED|incomplete|passed)]
upload_delete[userid,fileid]

Validation des entrées [INPUT]
input_validation_fail[:field,userid]

Comportement malveillant [MALICIOUS]
malicious_excess_404:[userid|IP,useragent]
malicious_extraneous:[userid|IP,inputname,useragent]
malicious_attack_tool:[userid|IP,toolname,useragent]
malicious_cors:[userid|IP,useragent,referer]
malicious_direct_reference:[userid|IP, useragent]

Changements de privilèges [PRIVILEGE]
privilege_permissions_changed:[userid,file|object,fromlevel,tolevel]

Modification des données sensibles [DATA]
sensitive_create:[userid,file|object]
sensitive_read:[userid,file|object]

sensitive_update:[userid,file|object]
sensitive_delete:[userid,file|object]

Erreurs de séquence [SEQUENCE]
sequence_fail:[userid]

Gestion des sessions [SESSION]
session_created:[userid]
session_renewed:[userid]
session_expired:[userid,reason]
session_use_after_expire:[userid]

Événements système [SYS]
sys_startup:[userid]
sys_shutdown:[userid]
sys_restart:[userid]
sys_crash[:reason]
sys_monitor_disabled:[userid,monitor]
sys_monitor_enabled:[userid,monitor]

Gestion des utilisateurs [USER]
user_created:[userid,newuserid,attributes[one,two,three]]
user_updated:[userid,onuserid,attributes[one,two,three]]
user_archived:[userid,onuserid]
user_deleted:[userid,onuserid]

ANNEXE 9 – LISTE DES CONTRÔLES DE SÉCURITÉS

(Document distinct)