

Gestion des risques de sécurité

09 juillet 2025

Points clés

- Le processus de gestion des risques de sécurité a été établi dans le cadre du système de gestion de la sécurité des Nations Unies (UNSMS) pour aider les organismes, les organisations, les fonds et les programmes des Nations Unies à identifier les événements néfastes futurs susceptibles d'affecter la réalisation des objectifs, à évaluer la probabilité et l'impact de ces événements, et à déterminer les mesures et interventions appropriées en matière de gestion des risques de sécurité.
- Le processus de gestion des risques de sécurité aide les responsables à évaluer les contextes d'intervention des Nations Unies, à identifier la mesure dans laquelle les menaces peuvent affecter le personnel, les actifs, les locaux et les opérations des Nations Unies, et à prendre les décisions appropriées en matière de gestion de la sécurité.
- Le processus de gestion des risques de sécurité permet aux utilisateurs de maximiser les possibilités offertes par les programmes à des niveaux de risque acceptables, tout en affectant les ressources nécessaires.
- Le processus de gestion des risques de sécurité est un mécanisme structuré comprenant neuf étapes consécutives.

1. Aperçu

Le processus de gestion des risques de sécurité est un processus analytique, établi dans le cadre de l'UNSMS, qui aide les organismes, les organisations, les fonds et les programmes des Nations Unies à identifier les événements néfastes futurs susceptibles d'affecter la réalisation des objectifs, à évaluer la probabilité et l'impact de ces événements, et à déterminer les interventions appropriées. Il aide les responsables à évaluer les contextes dans lesquels les Nations Unies interviennent, à identifier la mesure dans laquelle les menaces peuvent affecter le personnel, les actifs, les locaux et les opérations des Nations Unies, et à prendre les décisions appropriées en matière de gestion de la sécurité. La gestion des risques de sécurité permet une

évaluation nuancée des risques pesant sur le personnel, y compris ceux liés au profil d'une personne donnée. La gestion des risques de sécurité est importante, car, en affectant des ressources appropriées, elle permet d'optimiser les possibilités offertes par les programmes et de mettre en œuvre des programmes à des niveaux de risque acceptables. La présente section du Manuel du Haut-Commissariat des Nations Unies pour les réfugiés (HCR) pour les situations d'urgence fournit aux responsables et au personnel du HCR

des informations techniques sur la gestion des risques de sécurité de l'UNSMS. Elle présente les principaux concepts et termes de la gestion des risques de sécurité, parmi lesquels les notions de « menace », de « vulnérabilité », de « probabilité », d'« impact » et de « risque ». La présente section entend permettre aux responsables et au personnel d'acquérir les connaissances nécessaires pour qu'ils puissent influencer sur le processus de gestion des risques de sécurité de l'UNSMS afin de s'assurer que le HCR est en mesure de poursuivre la mise en œuvre des programmes, tout en maintenant les risques de sécurité qui pèsent sur le personnel, les locaux, les opérations et les actifs à un niveau acceptable pour rester en place et produire des résultats. Les responsables doivent toujours coordonner toutes les étapes de la gestion des risques de sécurité avec le responsable de la sécurité sur le terrain.

2. Pertinence pour les opérations d'urgence

Lorsque le HCR répond à des situations d'urgence, il peut être nécessaire de mener une gestion des risques de sécurité spécifique pour soutenir cette activité et/ou déterminer les risques pesant sur une zone dans laquelle les Nations Unies n'ont mené que peu d'activités auparavant, voire aucune. Si nécessaire, il est important d'entreprendre cette démarche en dehors du processus normal de gestion des risques de sécurité.

Remarque : dans les situations d'urgence, il est **fortement recommandé de réduire les délais, car les menaces et les risques pour le personnel et les opérations évoluent rapidement** et peuvent donc changer à brève échéance, nécessitant des ajustements soudains.

3. Conseils principaux

Définitions :

Menace : une cause potentielle de préjudice découlant d'actions délibérées. Une menace est une association d'intention, de capacité et de contexte inhibiteur.

Danger : une cause potentielle de préjudice résultant d'actions non délibérées.

Vulnérabilité : une faiblesse qui peut permettre à une menace ou à un danger de causer un préjudice.

Risque : l'association de la probabilité qu'un événement préjudiciable se produise et de l'impact de cet événement s'il se produit.

Probabilité : une évaluation de la possibilité qu'un événement préjudiciable affecte l'organisation.

Impact : une évaluation du préjudice potentiel qu'un événement (s'il se produisait) causerait à l'organisation.

Gestion des risques : la détermination et la mise en œuvre systématiques d'approches opportunes et efficaces pour gérer les effets des menaces pesant sur l'organisation.

Prévention : la prise de mesures visant à réduire la probabilité.

Atténuation : la prise de mesures visant à réduire l'impact.

Le processus de gestion des risques de sécurité

Le processus de gestion des risques de sécurité de l'UNSMS est un processus de gestion des risques propre au contexte qui identifie les menaces et les niveaux de risque associés ainsi que les interventions adéquates en matière de gestion des risques pour une prise de décision structurée en vue de s'accommoder des risques de sécurité. La gestion des risques de sécurité a été conçue de façon à être dynamique, réactive et souple afin de pouvoir s'adapter aux changements rapides de la situation ou du contexte sécuritaire et de la mise en œuvre des programmes. La gestion des risques de sécurité est également conçue pour intégrer des approches centrées sur les personnes au sein du processus, afin de veiller à ce que les évaluations des risques tiennent compte des différents profils individuels du personnel, et identifie les risques propres au contexte différenciés et les mesures d'atténuation qui doivent être mises en place pour garantir que le niveau de risque qui en résulte est acceptable pour tous. L'intégration d'une approche centrée sur les personnes au sein de la gestion des risques de sécurité permet à nos opérations de bénéficier d'un environnement favorable pour maintenir différents profils de personnel et soutenir les diverses communautés qui font l'objet d'interventions en tenant compte des nuances spécifiques au contexte.

Au niveau opérationnel, la direction du HCR et les équipes de sécurité sur le terrain contribuent activement au processus de gestion des risques de sécurité de l'UNSMS par l'identification, la portée, l'échelle et l'évaluation des activités programmatiques et de l'exposition potentielle aux menaces pour la sécurité et aux niveaux de risque, en veillant à ce que les mesures de gestion des risques de sécurité répondent aux besoins du HCR et soient adaptées et viables sur le plan opérationnel pour que l'organisation les mette en œuvre, et réduisent les risques de sécurité à des niveaux acceptables pour le HCR. Le processus se compose de neuf étapes, détaillées ci-après :

SECURITY RISK MANAGEMENT PROCESS

STEP 1: Geographical scope and timeframe

 Sets the terms of each SRM process by geography and timeframe. For example, a specific SRM may be completed for upcoming elections in a country, or for a specific area of potential vulnerability to be visited by United Nations staff, such as a large refugee camp.

STEP 2: Situational analysis

 Considers political, economic, social and environmental factors in each area, in relation to possible impacts on the safety and security of UN activities.

STEP 3: Programme assessment

 Formally identifies the goals and specific implementation activities of UNSMS organizations in-country.

STEP 4: Threat assessment

 Assesses actors and actions that may cause harm to the UNSMS in the Designated Area, in the categories of armed conflict, terrorism, crime and civil unrest. The intent and capabilities of the relevant threat actors are identified and assessed.

STEP 5: Security risk assessment

 Assesses the different vulnerabilities of the UNSMS presence and activities in-country against the existing threats to determine the likelihood of harmful threat event occurring, and possible impact on UNSMS personnel, assets and operations.



Étape 1. Portée géographique et délais

L'UNSMS détermine la portée géographique et les délais du processus de gestion des risques de sécurité, en définissant les emplacements géographiques afin de structurer le contexte dans lequel les évaluations des programmes et de la vulnérabilité sont réalisées. En général, les zones présentant des caractéristiques de sécurité similaires doivent être regroupées au sein de la même portée géographique désignée sous le terme de « zone de gestion des risques de sécurité ».

Une fois la portée géographique déterminée, il est important d'établir des délais clairs, afin de mieux définir les programmes, l'échelle, la portée, les acteurs présentant une menace, et ainsi la probabilité des menaces et leur impact sur les Nations Unies. La gestion des risques de sécurité peut faire l'objet de délais variés (de quelques heures à plus), mais le délai maximal autorisé est d'un an.

Il convient de noter que lorsqu'une opération d'urgence est considérée comme établie, un nouveau processus de gestion des risques de sécurité peut être justifié, car la zone géographique peut ne pas relever des processus de gestion des risques de sécurité existants.

Étape 2. Analyse de la situation

L'analyse de la situation fournit des informations contextuelles concises sur la zone de gestion des risques de sécurité pour que les décideurs en matière de sécurité comprennent le contexte opérationnel à travers différents thèmes, tels que la politique, l'économie, l'environnement, les infrastructures, les forces de sécurité, les groupes/acteurs présentant des menaces et le mandat des Nations Unies, qui sont pertinents pour la sûreté et la sécurité des Nations Unies dans la zone géographique évaluée.

Il s'agit d'un résumé pratique de ce à quoi « ressemble » la zone de gestion des risques de sécurité et de ce à quoi l'on peut s'attendre en matière d'environnement de travail. Cette partie du document est essentielle pour identifier les problèmes qui existent depuis longtemps et qui peuvent créer les conditions propices à l'émergence de menaces.

Remarque sur l'inclusion d'une approche centrée sur les personnes dans la gestion des risques de sécurité

Il est essentiel que dans le cadre de la section consacrée à l'analyse de la situation du processus de gestion des risques de sécurité, des recherches soient menées sur les considérations centrées sur les personnes et les incidents antérieurs (tendances) dans la zone de gestion des risques de sécurité, et de tenir compte de ces considérations :

1. Violence basée sur le genre ;
2. Perceptions concernant les personnes LGBTIQ+, ciblage de ces dernières et violence à leur rencontre ;
3. Identification des personnes en situation de handicap et discrimination à leur rencontre ;
4. Relations tribales, ethniques et intercommunautaires, et composition de la communauté, perceptions des différents groupes religieux dans la zone de gestion des risques de sécurité ;
5. Autres facteurs intersectionnels qui peuvent avoir une incidence sur les opérations ou le personnel des Nations Unies.

Il est essentiel de comprendre le contexte et la situation dans la zone de gestion des risques de sécurité, les tendances centrées sur les personnes en matière de violence basée sur le genre qui peuvent exister, la discrimination à l'égard de certains profils du personnel ainsi que les tensions préexistantes au sein des communautés pour pouvoir identifier de façon appropriée : 1) les menaces spécifiques contre le personnel du HCR, qui peuvent être prises en compte dans la partie « Évaluation des menaces » du processus et du document de gestion des risques de sécurité, et 2) les menaces qui pèsent sur les partenaires et les personnes relevant du mandat du HCR au nom desquelles le personnel du HCR chargé de la sécurité engagera des acteurs pertinents et travaillera avec d'autres unités pour identifier les mesures d'atténuation à prendre.

Étape 3. Évaluation des programmes

Une évaluation des programmes permet à un professionnel de la sécurité de comprendre de façon formelle les exigences des programmes des organisations de l'UNHCR, et met en évidence les programmes exposés à des menaces particulières. Les évaluations des programmes fournissent des informations générales et spécifiques sur les activités propres aux organismes menées au sein de la zone de gestion des risques de sécurité.

L'équipe opérationnelle de pays du HCR doit impérativement fournir des informations pertinentes et à jour au Département de la sûreté et de la sécurité des Nations Unies pour qu'il réalise une évaluation précise des programmes qui permettra à l'UNHCR de comprendre la portée et l'échelle des programmes et des opérations du HCR ainsi que les menaces et les risques potentiels auxquels sont exposés le personnel, les actifs, les opérations et les locaux du HCR. Par ailleurs, des programmes spécifiques peuvent faire face à des risques accrus par rapport à d'autres.

Par exemple :

- Les activités de suivi de la protection du HCR peuvent faire l'objet de menaces spécifiques en raison des informations sensibles sur les populations vulnérables et des actions des acteurs présentant des menaces, des autorités étatiques ou de fait, ou des groupes armés non étatiques.
- Compte tenu des modalités opérationnelles uniques du HCR, selon lesquelles les personnes contraintes de fuir rencontrent les équipes de protection dans les bureaux ou les locaux du HCR, le HCR est exposé à une probabilité accrue de troubles publics violents ou non violents, d'intrusions dans les infrastructures, d'occupation des locaux, etc.

Remarque sur l'inclusion d'une approche centrée sur les personnes dans la gestion des risques de sécurité

La partie « Évaluation des programmes » de la gestion des risques de sécurité doit également inclure une référence aux activités menées par le HCR et d'autres organismes de l'UNHCR qui peuvent être considérées comme augmentant l'exposition à un risque spécifique ou à la probabilité d'un ciblage, notamment les activités de protection, le travail avec les personnes LGBTIQ+, les campagnes de vaccination, l'autonomisation des femmes (dans les sociétés patriarcales) ou lorsque l'identité des membres du personnel chargés de la mise en œuvre du programme peut accroître le risque (âge, religion, appartenance ethnique ou tribale).

Il est essentiel d'être en mesure d'identifier les problèmes susceptibles de découler des activités programmatiques pour pouvoir affiner les menaces spécifiques à un stade ultérieur du processus de gestion des risques de sécurité.

Étape 4. Évaluation des menaces

Une évaluation des menaces identifie et évalue les acteurs et les actions dans une zone géographique donnée qui sont susceptibles de porter préjudice au système des Nations Unies. Les évaluations des menaces sont également divisées selon que les menaces sont générales ou spécifiques.

L'étape d'évaluation des menaces de la gestion des risques de sécurité se compose de deux

parties distinctes.

Une évaluation des menaces générales évalue et décrit de façon objective les menaces et les dangers en matière de sécurité dans l'environnement d'une zone de gestion des risques de sécurité (au sein de l'UNSMS, le concept de « sécurité » couvre les menaces et le concept de « sûreté » couvre les dangers. Cependant, le domaine de la « sûreté » de l'UNSMS ne couvre pas tous les dangers non délibérés. L'UNSMS poursuit une mission dans seulement trois domaines de la sûreté : sûreté des routes, à l'égard des incendies et dans le domaine aérien).

Chaque menace ou danger est évalué(e) sur une échelle de 1 à 5 selon trois variables :

- Intention : la motivation ou la disposition d'un acteur présentant une menace à concrétiser la menace.
- Capacité : la capacité ou l'aptitude des acteurs présentant une menace à concrétiser la menace.
- Contexte inhibiteur : les facteurs extérieurs aux Nations Unies dans la zone géographique qui entravent l'intention ou la capacité.

L'évaluation des menaces générales donne lieu à une note pour chaque type de menace ou de danger, et à un niveau de sécurité combinant la note de chaque menace et de chaque danger.



Évaluation des menaces spécifiques

Les évaluations des menaces spécifiques identifient les menaces spécifiques pesant sur les organismes, les organisations, les fonds et les programmes des Nations Unies dans une zone de gestion des risques de sécurité donnée. Contrairement aux évaluations des menaces générales qui demeurent génériques, les évaluations des menaces spécifiques identifient des menaces précises contre les Nations Unies en général ou un organisme en particulier au sein de la zone de gestion des risques de sécurité.

Pour procéder à une évaluation des menaces spécifiques, il est nécessaire de générer des descriptions d'événements complètes liées à la catégorie des menaces générales.

Une description d'événement est une description claire d'un événement préjudiciable que l'évaluation des risques de sécurité examinera en détail pour ensuite définir le niveau de risque. Elle doit aborder les effets négatifs de l'événement sur l'organisation et viser à répondre aux questions « Qui, Quoi, Quand, Où et Comment ».

Remarque : **les descriptions d'événements doivent fournir suffisamment d'informations pour affiner les paramètres**, en permettant aux décideurs d'évaluer les événements avec plus de précision qu'ils ne le feraient dans le cadre d'une évaluation des menaces générales.

- Tous les événements ne ciblent pas les Nations Unies. C'est pourquoi les descriptions d'événements doivent également préciser s'il s'agit d'une menace « directe » ou « indirecte ».
- **Les menaces directes identifient spécifiquement les Nations Unies.** Si un groupe particulier a déclaré qu'il avait l'intention de porter préjudice aux Nations Unies, par exemple, ou que l'histoire récente montre que les Nations Unies sont la cible de menaces, la menace doit être considérée comme « directe ».

« L'enlèvement d'un membre du personnel international des Nations Unies contre une rançon par des acteurs non étatiques sur le site X »

[Quoi] [Accent direct sur les Nations Unies] [Quoi] [Qui] [Où]

- **Les menaces indirectes désignent des menaces qui peuvent porter préjudice aux Nations Unies même si les Nations Unies ne sont pas nécessairement la cible principale.** Les Nations Unies peuvent être exposées à des préjudices si le personnel ou les actifs des Nations Unies se trouvent au mauvais endroit au mauvais moment, sont des victimes ou dommages collatéraux, sont associés à une cible ou si les Nations Unies se trouvent en travers du chemin par exemple.

« Un véhicule des Nations Unies frappé par un engin explosif improvisé sur la route X à destination du bureau de terrain Y »

[Accent indirect sur les Nations Unies] [Quoi/Comment] [Où]

Les menaces directes et indirectes peuvent être sous-divisées selon qu'il s'agit de menaces connues ou évaluées :

- Menaces connues : une déclaration d'intention de causer préjudice aux Nations Unies a été faite ou les Nations Unies ont déjà subi des préjudices.
- Menaces évaluées : aucune intention de causer préjudice n'a été déclarée, mais l'analyse ou les évaluations suggèrent l'existence d'une menace.

Une fois que les menaces spécifiques ont été identifiées et que les descriptions d'événements ont fait l'objet d'un consensus, une évaluation des menaces pour chaque événement est préparée, en s'appuyant sur l'évaluation de trois variables : l'intention de l'acteur/la partie responsable de la menace, la capacité de l'acteur/la partie responsable de la menace et le contexte inhibiteur de l'environnement dans lequel la menace survient (par exemple la capacité des forces de sécurité ou le rejet de tels actes par la population). Les évaluations des menaces spécifiques sont évaluées et notées de la même façon que les évaluations des menaces générales (voir plus haut).

Remarque : **ne pas fonder les évaluations et les décisions sur la menace mais sur le risque**. Dans chaque zone de gestion des risques de sécurité, il est possible d'identifier une menace grave (par sa nature) qui ne présente néanmoins qu'un faible risque pour les Nations Unies (voir plus bas la section relative au **risque**).

Remarque sur l'inclusion d'une approche centrée sur les personnes dans la gestion des risques de sécurité

Il est essentiel que le personnel de sécurité du HCR prenne part au processus collectif et s'assure que les menaces contre certains profils sont correctement prises en compte dans le processus de gestion des risques de sécurité. Par exemple :

1. La gestion des risques de sécurité identifie-t-elle une zone touchée par un conflit armé, par un effondrement de l'ordre public, par une criminalité élevée ou par des violences basées sur le genre généralisées ?
2. Des indicateurs contextuels ou des éléments déclencheurs liés à des profils de risque spécifiques du personnel ont-ils été pris en compte lors de l'identification des menaces ?

Par ailleurs, le personnel de sécurité du HCR veillera à ce que les descriptions d'événements s'appuient sur des informations relatives aux menaces recueillies et reflétées dans les parties précédentes du processus de gestion des risques de sécurité (c'est-à-dire l'analyse de la situation), qu'elles identifient les menaces pesant sur les activités détaillées dans l'évaluation des programmes, qu'elles soient formulées de façon spécifique et adéquate pour refléter la catégorie de personnel affectée, les profils individuels et les acteurs présentant une menace (qui, quoi et par qui) et qu'elles incluent les lieux et les moments précis où les menaces peuvent se concrétiser de façon à concevoir de façon adéquate (à un stade ultérieur du processus) les mesures de gestion des risques de sécurité visant à atténuer la probabilité et l'impact.

Étape 5. Évaluations des risques de sécurité

Une évaluation des risques de sécurité détermine et s'attache à quantifier la probabilité et l'impact des menaces, en tenant compte de la vulnérabilité des Nations Unies.

Probabilité

Dans le modèle de gestion des risques de sécurité, la probabilité est définie comme une évaluation de la possibilité qu'un événement préjudiciable affecte l'organisation. Il s'agit de la probabilité qu'un événement préjudiciable délibéré identifié se produise. Le descripteur de probabilité est un produit de la menace et de la vulnérabilité en matière de prévention. Des mesures de prévention sont prises pour réduire la probabilité qu'un événement préjudiciable donné se produise. Elles peuvent comprendre, entre autres, l'adoption d'itinéraires alternatifs, des contrôles d'accès, des mesures de dissuasion, la communication, des couvre-feux. Pour être efficaces, les mesures de prévention doivent être mises en œuvre avant que l'événement en question se produise.

La vulnérabilité en matière de prévention est définie comme l'absence de mesures de prévention visant à réduire la probabilité que l'événement se produise comme décrit. Les menaces étant

extérieures aux Nations Unies, les Nations Unies ne peuvent pas les contrôler facilement. Il s'agit de faire de son mieux en réduisant la vulnérabilité en matière de prévention et, ainsi, en diminuant la probabilité que les menaces se concrétisent.

La vulnérabilité en matière de prévention est évaluée sur une échelle de 1 à 5 selon les descripteurs suivants :

1. Des mesures et procédures de gestion des risques préventives efficaces sont pleinement en place et sont toujours efficaces.
2. Des mesures et procédures préventives efficaces sont pleinement en place mais présentent une faiblesse qui pourrait être exploitée.
3. Des mesures et procédures préventives ne sont pas pleinement en place OU ne sont pas toujours efficaces.
4. Des mesures et procédures préventives ne sont pas pleinement en place ET ne sont pas toujours efficaces.
5. Aucune procédure ni mesure préventive efficace n'est en place.

L'outil de gestion des risques de sécurité génère alors une note de probabilité en multipliant la menace et la vulnérabilité en matière de prévention :

- 1 - Très peu probable.
- 2 - Peu probable.
- 3 - Moyennement probable.
- 4 - Probable.
- 5 - Très probable.

Impact

L'impact est défini comme une évaluation du préjudice potentiel qu'un événement (s'il se produisait) causerait à l'organisation. Il couvre le personnel et les opérations. Il comprend également notre capacité à contrôler ou à réduire les effets secondaires d'un événement à travers la vulnérabilité en matière d'atténuation.

L'impact est le produit de trois éléments :

- Effet sur le personnel.
- Effet sur les opérations.
- Vulnérabilité en matière d'atténuation.

Une échelle de 1 à 5 est utilisée avec les descripteurs associés pour mesurer l'effet sur le personnel et les opérations.

Effet sur le personnel

1. Aucun effet.
2. Effet légèrement préjudiciable.
3. Effet modérément préjudiciable ou traumatisant sur le plan psychologique.
4. Effet gravement préjudiciable ou traumatisant sur le plan psychologique ou mortel (une

personne ou un petit nombre de personnes).

5. Effet mortel catastrophique (un grand nombre de victimes)

Effet sur les opérations

1. Aucun effet.
2. Effet légèrement perturbateur sur les programmes ou dommages légers aux actifs.
3. Effet gravement perturbateur sur les programmes ou dommages significatifs aux actifs.
4. Suspension des programmes à court ou moyen terme.
5. Suspension à long terme ou révocation des programmes.

Vulnérabilité en matière d'atténuation

La vulnérabilité en matière d'atténuation désigne l'absence de mesures et de procédures de sécurité visant à réduire l'impact d'un événement (si cet événement venait à se produire). Les mesures d'atténuation sont les mesures prises pour réduire l'impact. Elles peuvent comprendre l'évacuation sanitaire primaire et l'[évacuation sanitaire secondaire](#), les troussees médicales de secours et les troussees de premiers secours individuelles, la gestion des situations de prise d'otages, la préparation grâce à la liaison avec le gouvernement d'accueil, la planification des situations entraînant un grand nombre de victimes, les exercices, le relèvement à la suite d'une catastrophe, [la planification de la continuité des opérations](#), etc. Bien que les mesures d'atténuation visent à réduire l'impact des événements lorsqu'ils se produisent et par la suite, pour être efficaces, elles doivent être planifiées et mises en œuvre avant que ces événements se produisent.

Pour déterminer le niveau d'impact, il est essentiel d'évaluer le degré de mise en œuvre des mesures d'atténuation. À cette fin, le modèle de gestion des risques de sécurité applique une échelle de 1 à 5 fondée sur les descripteurs suivants :

1. Des mesures et procédures d'atténuation des risques sont pleinement en place et sont toujours efficaces.
2. Des mesures et procédures d'atténuation sont en place, mais peuvent ne pas toujours être efficaces ou peuvent avoir des limites.
3. Des mesures et procédures d'atténuation ne sont pas pleinement en place OU ne sont pas toujours efficaces.
4. Des mesures et procédures d'atténuation ne sont pas pleinement en place ET ne sont pas toujours efficaces.
5. Aucune mesure ni procédure d'atténuation n'est en place.

Le modèle de gestion des risques de sécurité additionne l'effet sur le personnel et les opérations à la vulnérabilité en matière d'atténuation pour déterminer l'impact (effet sur le personnel + effet sur les opérations + vulnérabilité en matière d'atténuation).

L'outil de gestion des risques de sécurité établit automatiquement une note d'impact selon une échelle de 1 à 5, comme suit :

- 1 - Négligeable.
- 2 - Mineur.

- 3 - Modéré.
- 4 - Grave.
- 5 - Critique.

Niveaux de risque

Une évaluation des risques associe les événements préjudiciables futurs susceptibles de se produire et la mesure dans laquelle ces événements peuvent porter préjudice à l'organisation.

Risque = probabilité x impact

Matrice de risque		Effet				
		Négligeable	Mineur	Modéré	Grave	Critique
P R O B A B I L I T É	Très probable	Faible	Moyenne	Élevée	Très élevée	Inacceptable
	Probable	Faible	Moyenne	Élevée	Élevée	Très élevée
	Moyennement probable	Faible	Faible	Moyenne	Élevée	Élevée
	Improbable	Faible	Faible	Faible	Moyenne	Moyenne
	Très improbable	Faible	Faible	Faible	Faible	Faible

En d'autres termes :

Fourchette de scores du risque	Niveau de risque
1 à 6	Faible
>6 à 10	Moyen
>10 à 16	Élevé
>16 à 20	Très élevé
>20 à 25	Inacceptable

Les niveaux de risque, qui sont les résultats finaux d'une évaluation des risques de sécurité, servent de base à la prise de décision dans le cadre du processus de gestion des risques de sécurité. Ils permettent aux décideurs d'élaborer les stratégies de gestion des risques adéquates et de fixer des priorités qui sont adaptées aux niveaux de risque et aux descriptions d'événements associées.

Remarque : afin de prendre des décisions **acceptables en matière de risques**, le niveau de risque le plus élevé associé à un événement donné s'applique à la zone de gestion des risques de sécurité ou à l'activité programmatique considérée.

Étape 6. Mesures de gestion des risques de sécurité

La gestion des risques passe par l'identification et la mise en œuvre des mesures de gestion des risques de sécurité qui réduisent la probabilité et/ou l'impact en atténuant les vulnérabilités.

Les mesures de gestion des risques de sécurité ne peuvent être identifiées qu'après avoir évalué

:

- Les forces et les faiblesses des mesures de prévention et d'atténuation existantes (en ce qui concerne des menaces spécifiques) ;
- Les niveaux de risque associés aux menaces, en fonction de leur probabilité et de leur impact ;

Dans le cadre des stratégies susmentionnées, les mesures de gestion des risques de sécurité peuvent être utilisées pour gérer les risques associés aux menaces identifiées. Une fois les vulnérabilités en matière de prévention et d'atténuation évaluées (comme décrit à l'étape précédente), les professionnels de la sécurité peuvent déterminer les mesures supplémentaires (des mesures qui ne sont pas actuellement en place) qui sont nécessaires, y compris les mesures et les procédures visant à réduire la probabilité ou l'impact, ou les deux. Ces décisions impliquent généralement de choisir la meilleure option parmi plusieurs possibilités.

Le processus de gestion des risques de sécurité vise à atteindre un équilibre entre l'impact des risques et le coût des solutions de sécurité conçues pour les gérer. Au moment de prendre des décisions, la capacité d'une mesure de sécurité à sauver des vies, et l'importance des programmes et des mandats en question sont des facteurs plus importants que le coût.

Remarque à l'attention des responsables. Ne pas fonder de décisions sur le niveau de menace. Décider des mesures à prendre une fois la vulnérabilité de l'organisation aux menaces établie. La gestion des risques tient compte aussi bien des coûts que des avantages : considérer les deux. Il est également important de tenir compte des coûts que représente la non-gestion d'un risque : ils peuvent être inacceptables, car non seulement les événements indésirables ont un impact principal, mais ils entraînent toujours des coûts secondaires et tertiaires pour l'organisation concernée.

Garder à l'esprit que la gestion des risques peut également permettre des économies en réduisant les pertes. Lors de la sélection des mesures de gestion des risques de sécurité possibles, il est important de tenir compte des éléments suivants :

- La mesure identifiée réduit en réalité le risque de la menace.
- Les impacts négatifs. Les tentatives de gestion d'un risque particulier peuvent malencontreusement en créer ou en accroître un autre. Par exemple, les longs contrôles d'accès qui retardent l'entrée dans les locaux peuvent exposer le personnel à une menace que les contrôles visaient à atténuer.
- Les coûts. Si la réparation des dommages causés par les menaces peut être coûteuse, elle peut améliorer la sécurité.
- Les ressources supplémentaires. Il convient d'inclure les coûts de formation, de soutien, de maintenance et d'autres facteurs qui sont nécessaires pour garantir que les mesures de gestion des risques de sécurité demeurent opérationnelles.
- Le temps nécessaire à la mise en œuvre. Lorsqu'il est question de contraintes de temps, plusieurs options doivent être étudiées. Pendant que les nouvelles mesures sont mises en place, des mesures provisoires peuvent être nécessaires pour combler des lacunes.

Une approche intégrée qui combine les aspects physiques, procéduraux, techniques et humains de la sécurité peut multiplier les avantages des mesures de gestion des risques de sécurité.

Basée sur les principes de dissuasion, de détection, de retardement et de prévention, cette approche est généralement désignée sous l'appellation « défense en profondeur », qui repose sur le concept de couches concentriques de sécurité. Lorsque les éléments composant un système de sécurité présentent plusieurs couches, ce dernier est plus difficile à déjouer.

Le processus de gestion des risques de sécurité est suffisamment souple pour garantir que les mesures peuvent être adaptées à une zone de gestion des risques de sécurité spécifique (si elle est différente de la zone désignée). Ainsi, il n'est pas nécessaire d'adopter les mêmes mesures minimales dans l'ensemble du pays. Ceci étant dit, les exigences qui sont obligatoires pour tous les lieux d'affectation – telles que la formation BSafe et les kits de démarrage pour le traitement préventif post-exposition (trousses de prophylaxie post-exposition) – doivent être satisfaites. Remarque sur l'inclusion d'une approche centrée sur les personnes dans la gestion des risques de sécurité

Les mesures de gestion des risques de sécurité doivent obligatoirement être centrées sur les personnes. Le personnel de sécurité doit collaborer avec la cellule de sécurité pour identifier des mesures adaptées, appropriées et réactives qui aident l'ensemble du personnel à réduire les risques à des niveaux acceptables. Le Manuel sur l'inclusion du genre dans la gestion de la sécurité et les directives sur la prise en compte du handicap dans la gestion de la sécurité décrivent en détail les facteurs à prendre en considération au moment d'identifier une mesure pour garantir une approche centrée sur les personnes. Parmi les éléments à prendre en compte figurent, entre autres, les points suivants :

1. Les mesures portent spécifiquement sur les descriptions d'événements identifiés et réduisent en particulier la probabilité et/ou l'impact de l'événement.
2. Les mesures soutiennent des catégories spécifiques de personnel aux profils divers. Par exemple, le personnel de l'UNSMS provenant d'une zone/tribu différente, des personnes d'une religion minoritaire, les femmes, les personnes LGBTIQ+, les personnes handicapées, les femmes enceintes, etc.
3. Les mesures proposées n'imposent pas de restrictions discriminatoires au personnel fondées sur le genre, l'orientation sexuelle, les caractéristiques sexuelles, et l'identité et l'expression de genre du personnel.

Le HCR est tenu de garantir la mise en œuvre de la page 22 du Manuel sur l'inclusion du genre dans la gestion de la sécurité et les pages 6 à 10 du chapitre XVI du Manuel des opérations de gestion de la sécurité consacré à la prise en compte du handicap dans la gestion de la sécurité.

Étape 7. Mise en œuvre de la gestion des risques de sécurité

Une fois que les mesures de sécurité ont été décidées et font l'objet d'un consensus, il convient de s'engager fermement à les mettre en œuvre dans les plus brefs délais. Lorsque les mesures et processus de gestion des risques sont approuvés au niveau approprié, ils deviennent des exigences. Un plan de mise en œuvre doit être élaboré pour s'assurer que les mesures sont mises en place et achevées efficacement et en temps opportun. Sans cette étape, le processus de gestion des risques de sécurité tout entier pourrait être voué à l'échec.

Les responsables doivent donc s'assurer que les acteurs de la sécurité et d'autres parties prenantes pertinentes (dont les ingénieurs, le personnel administratif, des technologies de

l'information et de la communication, de l'approvisionnement, etc.) adoptent une approche intégrée de la gestion de projets lorsqu'ils documentent la planification, l'organisation et les ressources nécessaires à la mise en œuvre efficace des mesures de gestion des risques de sécurité.

Les aspects suivants doivent être pris en compte :

- Mesures de prévention/d'atténuation. Préparer une liste détaillée et spécifique des mesures proposées.
- Objectif en matière de prévention/d'atténuation. Expliquer comment les mesures en question permettront de gérer les risques identifiés. Y parviendront-elles en réduisant la probabilité ou l'impact, ou les deux ?
- Ressources/coûts. Détailler les ressources nécessaires, y compris les coûts de financement et de coopération. Prendre en considération les coûts ponctuels et récurrents (pour la maintenance, la formation, etc.).
- Acteur responsable. Décider du responsable, de la personne ou de l'entité responsable de la mise en œuvre de chaque mesure.
- Délai. Fixer un délai réaliste pour la réalisation de chaque mesure et un délai pour l'achèvement du projet. Des mesures alternatives ou temporaires peuvent être nécessaires pour couvrir les lacunes jusqu'à la mise en œuvre complète.
- Mise à jour sur les avancées. Publier des mises à jour régulières sur le processus de mise en œuvre. Dresser la liste des mesures en attente et achevées, ainsi que les mesures supplémentaires requises. Introduire des mécanismes d'évaluation, de preuve et de validation.
- Budget. Déterminer si les mesures de gestion des risques de sécurité sont des mesures conjointes des Nations Unies ou si elles sont propres à l'organisation pour identifier le responsable du budget et obtenir l'autorisation budgétaire pour les mesures prévues.

Étape 8. Détermination du risque acceptable.

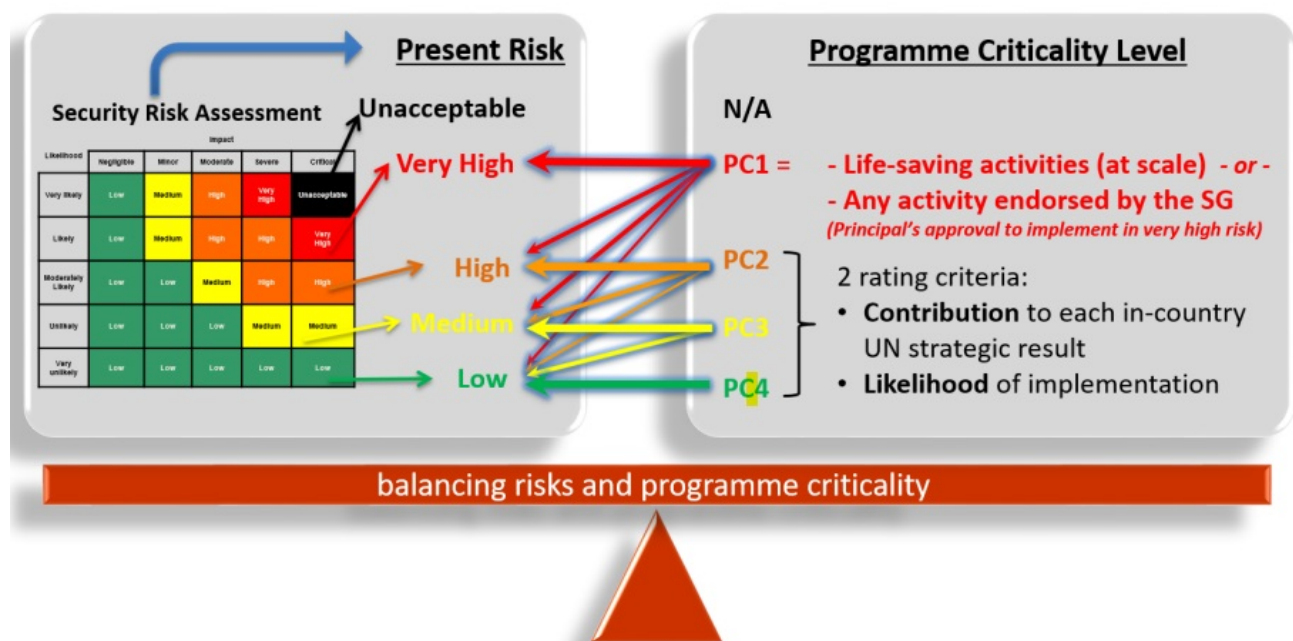
Bien que le processus de gestion des risques réduise les risques au moyen de mesures d'atténuation et de prévention (comme décrit dans les sections précédentes), tous les risques ne peuvent pas être complètement éliminés. Les principes ci-après guident l'UNSMS en ce qui concerne l'acceptabilité des risques.

- Ne pas accepter les risques inutiles. Accepter un risque ne procure aucun avantage si cela n'aide pas les Nations Unies à atteindre ses objectifs.
- Accepter les risques lorsque les avantages dépassent les risques. Bien que tous les risques ne puissent pas être éliminés, éviter tous les risques n'aide pas les Nations Unies à atteindre ses objectifs.
- Prendre des décisions de gestion des risques au bon niveau. Les organisations doivent veiller à ce que les décisions relatives aux risques soient prises au niveau de l'autorité. Les responsables et le personnel ne doivent pas supposer qu'un risque n'a pas été dûment autorisé.
- Il convient de prendre toutes les mesures raisonnables pour réduire les risques. Il importe de toujours essayer de diminuer les risques dans la mesure du possible, même si un certain degré de risque est accepté.

Modèle des risques acceptables

Le modèle des risques acceptables de l'UNSMS vise un équilibre entre les risques de sécurité et les avantages des programmes (appelé « [criticité des programmes](#) »). Pour évaluer l'acceptabilité des risques, quatre niveaux de [criticité des programmes](#) sont examinés par rapport aux niveaux de risque générés à l'étape 5 ci-dessus (Évaluation des risques de sécurité). Le modèle des risques acceptables fait la distinction entre les activités réalisées par les partenaires d'exécution et les activités menées par le personnel des Nations Unies, et ne traite que de ces dernières. Il établit le niveau maximal de risque de sécurité qui est acceptable pour chaque niveau de criticité des programmes. Un outil distinct de [criticité des programmes](#) est utilisé pour établir les niveaux de [criticité des programmes](#) pour les activités impliquant du personnel des Nations Unies.

Il existe un niveau de risque (niveau le plus élevé de probabilité et niveau le plus élevé d'impact) qui n'est pas acceptable, quelle que soit l'importance de l'activité que le personnel des Nations Unies souhaite mener. Le tableau ci-après établit la relation existant entre le risque acceptable, la criticité des programmes et la responsabilité décisionnelle. (Il part du principe que l'organisation a pris toutes les mesures possibles pour diminuer les risques de sécurité.)



Activités de niveau 1 de criticité des programmes uniquement dans des environnements où le risque actuel est très élevé ;

Niveaux 1 et 2 de criticité des programmes dans des environnements où le risque actuel est élevé

Niveaux 1, 2 et 3 de criticité des programmes dans des environnements où le risque actuel est moyen

Niveaux 1, 2, 3 et 4 de criticité des programmes dans des environnements où le risque est faible

Étape 9. Suivi et évaluation

L'objectif du suivi et de l'évaluation est d'améliorer l'efficacité des mesures de gestion des risques de sécurité et de permettre la mise en œuvre d'un nombre croissant de programmes à un niveau de risque acceptable. Le suivi fournit des indications quant aux progrès accomplis ou non dans la mise en œuvre des mesures de gestion des risques de sécurité. C'est ce que l'on appelle généralement la « conformité ». Les évaluations sont essentielles pour garantir que la gestion des risques de sécurité est adaptée aux objectifs fixés.

Liste de contrôle

- Comprendre la structure de sécurité des Nations Unies et les principaux acteurs (responsable désigné, coordonnateur de secteur [sécurité], équipe de coordination du dispositif de sécurité/équipe de coordination du dispositif de sécurité de la zone) ainsi que le personnel de sécurité du HCR de l'opération qui ont tous un rôle clé à jouer dans la mise en œuvre du processus de gestion des risques de sécurité.
- Soutenir activement la réalisation de la gestion des risques de sécurité. Veiller à la mise en œuvre et à l'intégration de l'approche centrée sur les personnes dans les processus de gestion des risques de sécurité pour s'assurer que les risques menaçant le HCR sont acceptables pour tous.
- Procéder à l'évaluation de la criticité des programmes conjointement à d'autres organismes des Nations Unies et utiliser les informations ainsi collectées pour soutenir la planification opérationnelle.
- Garantir que les risques identifiés dans le cadre de la gestion des risques de sécurité sont également reflétés dans le registre des risques de l'opération et que le traitement des risques correspond aux mesures de gestion des risques de sécurité.

4. Politiques et lignes directrices

5. Liens

[« Security Policy Manual - UN Security Management System » \(Manuel sur les poli... « Risk Management - Duty of Care, occupational health, safety and security » \(G...](#)

6. Contacts principaux

Service de la sécurité sur le terrain du HCR, Division des urgences, de la sécurité et de l'approvisionnement (DESS). À l'adresse : FS00@unhcr.org