ACADÉMIE HUMANITAIRE · HUMANITAIRES JOBS

Mini MBA Sécurité et gestion des risques : protéger les équipes et garder l'accès

Support de cours · Semaine 3 : Évaluer les risques : menaces, vulnérabilités, probabilité et impact

Programme de 3 mois exactement (12 semaines, 144 heures) pour gérer la sécurité et les risques d'une organisation humanitaire : devoir de protection, analyse du contexte, évaluation des risques, plans et procédures, acceptation et négociation de l'accès, incidents, gestion de crise et enlèvement, santé et bien-être du personnel, sécurité numérique et protection des données, risques de l'organisation et conformité, partage du risque avec les partenaires, gouvernance et continuité d'activité. Exercices chiffrés corrigés, trois examens mensuels avec études de cas, et un diplôme vérifiable de l'Académie Humanitaire.

https://humanitairejobs.org/fr/academie/mini-mba-securite-risques/semaine-3/

Document gratuit de l'Académie Humanitaire. Il peut être imprimé et partagé librement à des fins de formation, sans modification.

Semaine 3 : Évaluer les risques : menaces, vulnérabilités, probabilité et impact

Objectifs

- Identifier les menaces et évaluer la vulnérabilité de l'organisation et de chaque profil de personnel face à elles.
- Noter les risques sur une matrice probabilité × impact, calculer le risque résiduel après mesures et le comparer au seuil acceptable.
- Rédiger une évaluation des risques claire, datée, révisable, qui conduit à des décisions.

Menace, vulnérabilité, risque

Trois notions à ne pas confondre :

- **Menace** : ce qui peut causer un dommage (braquage de véhicule, enlèvement, bombardement, engin explosif, émeute, maladie, accident de la route).
- **Vulnérabilité** : le degré d'exposition de l'organisation ou d'une personne à cette menace, selon sa localisation, ses déplacements, son profil, ses biens, ses procédures, son acceptation.
- **Risque** : la combinaison de la probabilité qu'une menace se réalise contre nous et de l'impact si elle se réalise.

Une même menace ne crée pas le même risque pour tous. **Exemple :** la menace d'enlèvement contre rançon pèse davantage sur les profils perçus comme « rentables » (personnel international de certaines nationalités, cadres nationaux de haut niveau, personnes dont la famille est perçue comme aisée). La vulnérabilité dépend aussi des procédures : des déplacements prévisibles, toujours aux mêmes heures, augmentent la vulnérabilité de tous.

La matrice probabilité × impact

La méthode la plus répandue note chaque risque sur deux échelles de 1 à 5 :

- **Probabilité** : 1 très improbable, 2 improbable, 3 possible, 4 probable, 5 très probable (sur une période définie, par exemple 12 mois).
- **Impact** : 1 négligeable, 2 mineur (dommages matériels limités), 3 modéré (blessures légères, interruption courte), 4 grave (blessures graves, perte de biens importants, suspension), 5 critique (décès, enlèvement, retrait du pays).

Score = probabilité × impact, de 1 à 25. Niveaux usuels : 1 à 4 faible, 5 à 9 moyen, 10 à 16 élevé, 20 à 25 très élevé (les seuils varient selon les organisations et doivent être écrits).

Menace	Probabilité	Impact	Score	Niveau
Braquage de véhicule sur l'axe nord	4	4	16	Élevé
Cambriolage du bureau	3	2	6	Moyen
Enlèvement d'un employé	2	5	10	Élevé
Accident de la route grave	3	5	15	Élevé

Remarque : l'accident de la route a souvent un score aussi élevé que les menaces liées à la violence, et il est plus facile à réduire.

Risque résiduel et seuil acceptable

Le **risque inhérent** est le risque avant mesures ; le **risque résiduel** est celui qui reste après les mesures prévues. La décision se prend sur le risque résiduel, comparé au seuil acceptable fixé par la direction pour l'activité considérée.

Exemple. Braquage sur l'axe nord : inhérent 4 × 4 = 16. Mesures : déplacements en deux véhicules, horaires variables, pas d'argent ni de biens de valeur visibles, communication avec contrôle d'appel toutes les heures, mise à jour quotidienne de l'état de la route par le forum des ONG, règle de non-résistance. Probabilité estimée réduite à 2 (la vulnérabilité baisse), impact réduit à 3 (non-résistance, assistance rapide). Résiduel : 2 × 3 = 6, niveau moyen.

Si le seuil acceptable pour les activités de distribution est « moyen », l'activité peut se poursuivre avec ces mesures. Si les mesures ne permettent pas de descendre sous le seuil, il faut changer l'activité (modalité, lieu, partenaire) ou la suspendre.

> Une mesure inscrite mais non appliquée ne réduit aucun risque. L'évaluation doit dire qui applique quoi, et comment on le vérifie.

Les limites de la notation

La matrice est utile mais trompeuse si on la prend pour une mesure exacte :

- Les notes sont des **jugements**, pas des mesures. Deux personnes peuvent noter différemment ; on cherche un consensus argumenté, avec le personnel national.
- Les **événements rares et catastrophiques** (attaque d'un hôtel, attentat contre une base) ont une faible probabilité mais un impact extrême : un score de 1 × 5 = 5 les classe « moyens » alors qu'ils exigent des plans spécifiques.
- Les risques **cumulés** : plusieurs risques moyens combinés peuvent constituer une situation inacceptable.
- Les risques évoluent : une évaluation non datée ou vieille de huit mois en contexte instable n'a plus de valeur.

Bonne pratique : garder un œil particulier sur toute menace d'impact 5, quelle que soit sa probabilité, et prévoir pour chacune un plan de contingence (enlèvement, attaque armée,

évacuation médicale).

Profils et sécurité inclusive

Les personnes ne sont pas exposées de la même manière selon leur **profil** : nationalité, origine ethnique ou clan, religion, genre, orientation sexuelle et identité de genre, handicap, âge, apparence, langue. Un même lieu peut être sûr pour l'un et dangereux pour l'autre.

Une approche **inclusive** de la sécurité (développée notamment par le GISF) consiste à :

- prendre en compte les profils dans l'évaluation des risques, sans obliger personne à révéler des informations personnelles ;
- permettre à chacun de signaler confidentiellement des préoccupations liées à son profil ;
- adapter les mesures (hébergement, déplacements, affectations), sans exclure automatiquement des personnes de certains postes ;
- former les responsables à ces questions.

Exemple. Un employé national d'un groupe ethnique minoritaire ne peut pas franchir certains points de contrôle sans risque. Plutôt que de l'exclure du projet, l'équipe adapte les itinéraires, l'affecte à des zones où son profil n'est pas exposé, et prévoit un hébergement sûr en cas de tension.

Rédiger l'évaluation

Une évaluation des risques de sécurité utile contient :

- la **zone** et la **période** couvertes, la date et les auteurs ;
- un résumé du contexte (renvoi à l'analyse) ;
- le tableau des menaces avec probabilité, impact, score inhérent ;
- pour chaque risque élevé ou très élevé : mesures, responsables, risque résiduel ;
- la comparaison au seuil acceptable par type d'activité ;
- les décisions et recommandations (poursuite, adaptation, suspension) ;
- la date de prochaine révision et les déclencheurs de révision anticipée.

Elle est **validée** par le directeur pays (et par le siège au-delà d'un certain niveau de risque) et **expliquée** au personnel concerné. Elle sert aussi de base au budget de sécurité et au consentement éclairé du personnel.

Exercice d'application : évaluer et décider

Situation. Une ONG veut ouvrir une base dans une ville à 120 km de la capitale régionale. Menaces identifiées : braquage de véhicule (probabilité 4, impact 4) ; attaque armée contre la base (probabilité 2, impact 5) ; enlèvement (probabilité 2, impact 5) ; accident de la route (probabilité 4, impact 4) ; maladie grave sans accès aux soins (probabilité 3, impact 4). Seuil acceptable fixé par la direction pour des activités de santé vitales : résiduel « élevé » au maximum (≤ 16), avec plan de contingence pour toute menace d'impact 5. Mesures proposées : convois de deux véhicules et contrôle d'appel (braquage ramené à 2 × 3), consignes routières et chauffeurs formés (accident ramené à 2 × 4), gardes non armés, mur et abri (attaque ramenée à 1 × 5), évacuation médicale par un service aérien contractualisé et trousses (maladie ramenée à 2 × 3). Aucune mesure spécifique pour l'enlèvement.

Travail demandé. 1) Scores inhérents et résiduels. 2) L'ouverture est-elle acceptable ? 3) Que manque-t-il ?

Corrigé. 1) Inhérents : braquage 16, attaque 10, enlèvement 10, accident 16, maladie 12. Résiduels : braquage 6, attaque 5, enlèvement 10 (inchangé), accident 8, maladie 6. 2) Tous les résiduels sont ≤ 16, donc dans le seuil, mais deux menaces d'impact 5 (attaque, enlèvement) exigent un plan de contingence. 3) Il manque des mesures et un plan pour l'enlèvement : analyse des profils exposés, discrétion des déplacements, variation des horaires, règles sur les visiteurs, préparation d'une cellule de crise et d'une politique de gestion des enlèvements ; et un plan de contingence en cas d'attaque (abri, communications de secours, procédure de relocalisation). L'ouverture peut être décidée une fois ces plans en place, validés par la direction.

À retenir

- Risque = probabilité × impact d'une menace, selon la vulnérabilité de l'organisation et des personnes.
- Décider sur le risque résiduel, comparé au seuil acceptable de l'activité.
- Une mesure non appliquée ne réduit rien : responsables et vérification obligatoires.
- Toute menace d'impact 5 exige un plan de contingence, quelle que soit sa probabilité.
- Sécurité inclusive : intégrer les profils sans exclure ni forcer la divulgation.

Quiz

1. Probabilité 3, impact 5. Le score est :
   A. 8
   B. 35
   C. 2
   D. 15

2. Après mesures, un risque passe de 4 × 4 à 2 × 3. Le risque résiduel est :
   A. 16
   B. 10
   C. 6
   D. 8

3. Une menace de probabilité 1 et d'impact 5 (score 5) :
   A. Peut être ignorée
   B. Exige un plan de contingence spécifique
   C. Est automatiquement acceptable
   D. Doit être notée 25

4. La décision de poursuivre une activité se prend sur :
   A. Le risque résiduel comparé au seuil acceptable
   B. Le risque inhérent
   C. L'avis du bailleur
   D. Le nombre d'incidents de l'an passé

5. Dans une approche de sécurité inclusive, on :
   A. Exclut automatiquement certains profils
   B. Oblige chacun à déclarer son orientation sexuelle
   C. Ignore les profils
   D. Permet des signalements confidentiels et adapte les mesures

Corrigé du quiz : 1. D · 2. C · 3. B · 4. A · 5. D