ACADÉMIE HUMANITAIRE · HUMANITAIRES JOBS

Mini MBA humanitaire : diriger une organisation humanitaire

Support de cours · Semaine 10 : Gestion des risques de l'organisation et de la sécurité

Programme de direction de 3 mois exactement (12 semaines, 144 heures) : leadership, stratégie, cycle de projet, MEAL, finance et budgets bailleurs, conformité et fraude, levée de fonds, supply chain, RH et safeguarding, risques et sécurité, négociation et plaidoyer, changement et gouvernance. Exercices chiffrés corrigés, trois examens mensuels exigeants avec études de cas, et un diplôme vérifiable de l'Académie Humanitaire.

https://humanitairejobs.org/fr/academie/mini-mba-humanitaire/semaine-10/

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

Semaine 10 : Gestion des risques de l'organisation et de la sécurité

Objectifs

- Mettre en place une gestion des risques à l'échelle de l'organisation : registre, appétence au risque, risques résiduels, partage des risques avec bailleurs et partenaires.
- Diriger la gestion des risques de sécurité : analyse de contexte, menaces, vulnérabilités, stratégies d'acceptation, de protection et de dissuasion.
- Préparer et conduire la gestion d'incidents critiques : cellule de crise, communication, continuité des activités.

La gestion des risques de l'organisation

La norme **ISO 31000** définit le risque comme l'effet de l'incertitude sur les objectifs. Une organisation humanitaire fait face à des risques de plusieurs natures : **sécurité**, **fiduciaires** (fraude, corruption, détournement), **juridiques et de conformité** (sanctions, droit du travail, protection des données), **opérationnels** (accès, rupture d'approvisionnement), **de réputation**, **éthiques** (abus, atteinte aux principes) et **financiers** (change, trésorerie, dépendance aux bailleurs).

Le **registre des risques** décrit chaque risque (cause, événement, conséquence), sa probabilité et son impact (souvent sur une échelle de 1 à 5), les mesures existantes, le **risque résiduel**, le responsable et la date de revue. Le niveau de risque est souvent calculé comme probabilité × impact : un risque de probabilité 4 et d'impact 5 obtient 20 sur 25, au-dessus d'un seuil d'escalade fixé par exemple à 15.

L'**appétence au risque**, approuvée par le conseil d'administration, dit quels risques l'organisation accepte pour remplir sa mission. Une ONG médicale peut accepter un risque de sécurité élevé pour soigner en zone de conflit, mais n'accepter aucun risque de tolérance envers l'exploitation sexuelle. Sans appétence au risque formalisée, chaque décision dépend de la personnalité du directeur en poste.

> Le **transfert des risques** vers les partenaires locaux est une dérive dénoncée par de nombreuses études : l'ONG internationale reste à l'abri tandis que son partenaire porte le danger sans moyens. Le **partage des risques** suppose de financer la sécurité des partenaires, de partager l'information et de décider ensemble de ce qui est acceptable.

Analyse des risques de sécurité

La gestion des risques de sécurité suit un cycle : **analyse de contexte** (acteurs, dynamiques du conflit, criminalité, perception de l'organisation), **identification des menaces** (enlèvement, attaque armée, braquage sur la route, engins explosifs, violence sexuelle,

détention arbitraire, troubles civils, catastrophes naturelles, maladies), **analyse des vulnérabilités** et des capacités, puis évaluation du risque et choix des mesures.

Une formule pédagogique résume la logique : **risque = menace × vulnérabilité / capacités**. On ne contrôle presque jamais la menace ; on agit sur la vulnérabilité (exposition, profil, routines prévisibles) et sur les capacités (formation, communications, procédures, réseau).

Le **seuil de risque acceptable** se décide en mettant en balance le risque résiduel et la **criticité du programme** : plus l'activité sauve des vies, plus un risque élevé peut être accepté, avec des mesures renforcées. Le cadre de criticité des programmes du système de l'ONU (Programme Criticality) et la démarche de l'organisation GISF (Global Interagency Security Forum) formalisent ce raisonnement.

Les sources d'information doivent être croisées : réseau de contacts locaux, forums de sécurité des ONG et organisations de conseil en sécurité, agences de l'ONU, médias locaux, données publiques sur les conflits (par exemple le programme de données sur les conflits d'Uppsala, UCDP). Les informations sensibles reçues de partenaires ou de tiers ne se rediffusent pas sans leur accord.

Stratégies : acceptation, protection, dissuasion

Le **triangle de la sécurité** distingue trois stratégies complémentaires :

- **Acceptation** : réduire ou supprimer la menace en obtenant le consentement des acteurs (communautés, autorités, groupes armés) grâce à la qualité, à l'impartialité perçue, à la transparence et au dialogue. C'est la stratégie privilégiée des ONG, mais elle se construit dans le temps et peut s'effondrer vite si un acteur juge l'organisation partiale.
- **Protection** : réduire la vulnérabilité par des mesures physiques et procédurales (murs, gardes, véhicules adaptés, procédures de déplacement, hibernation, réduction de la visibilité).
- **Dissuasion** : opposer une contre-menace (escortes armées, retrait conditionnel, pression politique). Les escortes armées sont en principe un dernier recours, encadré par les directives de l'IASC sur les escortes armées, car elles peuvent compromettre la neutralité perçue et créer de nouveaux risques.

Le **plan de sécurité** d'un pays comprend : analyse des risques, niveaux de sécurité et indicateurs de passage d'un niveau à l'autre, procédures standard (déplacements, communications, gestion de l'argent liquide, visiteurs), plans de contingence (hibernation, relocalisation, évacuation) et organigramme de crise. Il doit être connu, compris et testé par des exercices, sinon il ne sert à rien.

> Indicateurs de déclenchement : décidez à l'avance quels événements font passer d'un niveau à l'autre (par exemple deux incidents armés à moins de 20 km de la base en une semaine). Sans indicateurs, la décision de relocaliser arrive souvent trop tard.

Gestion des incidents critiques

Un **incident critique** (enlèvement, décès, agression grave, attaque d'un bureau, disparition) dépasse les capacités normales de gestion. Il est géré par une **équipe de gestion de crise** au siège ou au niveau régional, distincte de l'équipe sur place, avec des rôles définis à l'avance : responsable de la crise, liaison avec la famille, communication, sécurité, juridique et assurance, ressources humaines, soutien psychologique.

Principes pour les premières heures : **sécuriser** les personnes encore exposées, **vérifier** les faits, **activer** la cellule de crise, **tenir un journal** chronologique de toutes les décisions et informations, **contrôler la communication** (aucune déclaration publique ni publication sur les réseaux sociaux par le personnel, un seul porte-parole), **informer la famille** avant tout autre public, et **coordonner** avec les autorités et les autres organisations.

En cas d'enlèvement, les organisations s'appuient sur des spécialistes et sur leurs assurances ; les politiques varient sur le paiement de rançons, interdit ou fortement découragé par plusieurs États et contraire aux régimes de sanctions dans certains cas. La politique de l'organisation doit être claire avant l'incident, pas improvisée pendant.

Après l'incident : soutien psychologique pour les personnes touchées et l'équipe, retour d'expérience sans recherche de bouc émissaire, mise à jour de l'analyse des risques et, le cas échéant, révision de la présence dans la zone.

Continuité des activités et réputation

La **continuité des activités** prépare l'organisation à continuer ses fonctions essentielles malgré une perturbation : perte d'un bureau, coupure des communications ou des banques, épidémie, cyberattaque, suspension de l'enregistrement. Le plan identifie les **fonctions critiques** (paie, paiements aux bénéficiaires, approvisionnements vitaux, communication avec les bailleurs), leur délai maximal d'interruption acceptable, et les solutions de repli (sauvegardes hors site, comptes bancaires alternatifs, délégations de signature, gestion à distance).

La **gestion à distance** (programmes conduits par des équipes nationales ou des partenaires quand le personnel de direction ne peut plus accéder à la zone) exige une attention particulière : transfert réel des moyens de sécurité, systèmes de suivi par des tiers, appels de vérification aux bénéficiaires, et vigilance pour ne pas transférer le risque sans transférer les moyens.

Le **risque de réputation** découle souvent des autres risques : un scandale d'abus, une fraude dissimulée ou un incident mal géré coûtent bien plus que leurs pertes directes. La meilleure protection est la transparence : informer les bailleurs et, quand c'est approprié, le public, de façon factuelle et rapide, en montrant les mesures prises.

La **cybersécurité** et la protection des données sont désormais des risques majeurs : authentification à deux facteurs, sauvegardes, mises à jour, formation contre l'hameçonnage, et chiffrement des données sensibles des bénéficiaires.

Exercice d'application : registre des risques et décision de relocalisation

Partie 1. Établissez un registre pour cinq risques de votre organisation (au moins un de sécurité, un fiduciaire, un de réputation, un de protection des données, un financier) : description cause-événement-conséquence, probabilité et impact sur 5, score, mesures existantes, risque résiduel, responsable. Indiquez lesquels dépassent un seuil d'escalade de 15.

Partie 2. Votre base de Morongo est au niveau de sécurité 3 sur 4. En dix jours : deux braquages de véhicules d'ONG sur l'axe principal, des tracts hostiles aux organisations étrangères, et l'annonce d'une opération militaire dans les 15 jours. La base gère un programme nutritionnel qui soigne 600 enfants en malnutrition aiguë sévère. Analysez la situation (menaces, vulnérabilités, criticité) et proposez une décision argumentée : maintien avec mesures, réduction des effectifs, gestion à distance ou relocalisation. Précisez les indicateurs qui déclencheraient l'étape suivante et la façon d'assurer la continuité des soins.

Éléments de corrigé. La criticité est très élevée (traitement vital d'enfants), ce qui justifie d'accepter un risque plus élevé, mais pas de s'exposer sans mesures. Une réponse solide réduit l'exposition (personnel non essentiel relocalisé, déplacements limités et non prévisibles, visibilité réduite), renforce l'acceptation (dialogue avec les leaders sur les tracts), prépositionne trois mois de produits nutritionnels, transfère progressivement la continuité des soins aux structures de santé et aux agents communautaires, et fixe des indicateurs clairs de relocalisation complète (combats à moins d'une distance donnée, menace directe contre l'organisation, impossibilité de communiquer).

À retenir

- Registre des risques : cause, événement, conséquence, probabilité × impact, risque résiduel, responsable, revue.
- Appétence au risque approuvée par le conseil ; partager les risques avec les partenaires, ne pas les transférer.
- Risque = menace × vulnérabilité / capacités ; le seuil acceptable dépend de la criticité du programme.
- Acceptation, protection, dissuasion ; escortes armées en dernier recours.
- Incident critique : cellule de crise, journal des décisions, un seul porte-parole, la famille informée en premier.

Quiz

1. Un risque de fraude a une probabilité de 3 et un impact de 4 ; un risque d'enlèvement une probabilité de 2 et un impact de 5. Les risques dont le score atteint ou dépasse 12 sont escaladés. Lesquels ?
   A. Aucun
   B. La fraude seulement (12), l'enlèvement est à 10
   C. L'enlèvement seulement
   D. Les deux

2. Organiser des rencontres régulières avec les chefs communautaires pour expliquer les critères de ciblage relève de la stratégie :
   A. De dissuasion
   B. De protection
   C. D'acceptation
   D. De transfert du risque

3. Après un enlèvement, la première personne à informer, avant tout communiqué public, est :
   A. Les journalistes
   B. La famille de la personne enlevée, par la personne désignée de la cellule de crise
   C. Les bailleurs
   D. Les réseaux sociaux de l'organisation

4. Pourquoi fixer à l'avance des indicateurs de passage d'un niveau de sécurité à l'autre ?
   A. Pour satisfaire les bailleurs
   B. Pour que la décision de réduire ou relocaliser ne dépende pas de l'humeur du moment et ne soit pas prise trop tard
   C. Pour éviter de former le personnel
   D. Parce que c'est exigé par la loi

5. Une ONG internationale confie à un partenaire local les activités d'une zone devenue trop dangereuse pour son propre personnel, sans budget de sécurité supplémentaire. C'est :
   A. Une bonne pratique de localisation
   B. Un transfert de risque, contraire au partage équitable des risques
   C. Une stratégie de dissuasion
   D. Une obligation des bailleurs

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