ACADÉMIE HUMANITAIRE · HUMANITAIRES JOBS

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

Support de cours · Semaine 12 : Gouvernance, culture de sécurité, continuité d'activité et projet final

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-12/

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

Semaine 12 : Gouvernance, culture de sécurité, continuité d'activité et projet final

Objectifs

- Organiser la gouvernance des risques : politique, rôles du conseil et de la direction, rapports, audits.
- Développer une culture de sécurité où chacun signale, apprend et protège l'acceptation.
- Construire un plan de continuité d'activité, et réaliser le projet final : un cadre de gestion des risques pour un pays.

La politique de sécurité et de gestion des risques

La **politique**, adoptée par le conseil, fixe le cadre que tous les pays et services appliquent :

- principes (devoir de protection, acceptation, droit de retrait, égalité de traitement, non-paiement aux parties au conflit) ;
- appétit pour le risque et seuils par catégorie ;
- rôles et responsabilités, de la direction aux points focaux ;
- exigences minimales : évaluation des risques, plan de sécurité, formation, signalement des incidents, gestion de crise ;
- position sur les questions sensibles (escortes armées, gardes armés, rançons, communication en cas d'enlèvement) ;
- suivi : rapports, audits, révisions.

Des **normes minimales** par niveau de risque rendent la politique opérationnelle. **Exemple :** dans tout pays classé à risque élevé, un conseiller sécurité dédié, un plan révisé tous les 6 mois, une formation avancée pour tout le personnel exposé, un exercice de crise annuel et des communications satellitaires dans chaque base.

Le rôle du conseil et de la direction

Le **conseil d'administration** ne gère pas la sécurité au quotidien, mais il en porte la responsabilité ultime :

- il adopte la politique et l'appétit pour le risque ;
- il reçoit un rapport régulier (au moins annuel, trimestriel pour les risques majeurs) ;
- il est informé sans délai des incidents graves et des crises ;
- il vérifie que les ressources sont suffisantes et que les audits sont suivis.

La **direction** rend des comptes avec un tableau de bord simple : incidents par catégorie et gravité, taux pour 100 employés, pays au-dessus du seuil, conformité aux normes minimales (plans à jour, formations, exercices), recommandations en retard, maturité.

Exemple de lecture. 12 pays ; 10 ont un plan de sécurité à jour (83 %) ; 7 ont fait un exercice de crise dans l'année (58 %) ; 3 pays ont des risques résiduels au-dessus de l'appétit. Le conseil demande pour ces 3 pays une décision explicite : mesures supplémentaires, réduction d'activités, ou acceptation motivée et temporaire du dépassement.

Auditer la sécurité

Les **audits de sécurité** (internes, par des pairs ou externes) vérifient que le dispositif existe et fonctionne :

- documents : évaluation des risques, plan, procédures, listes de contacts, journal des incidents ;
- pratiques : contrôles d'appel effectifs, carnets de mouvements, registres de visiteurs, tests radio ;
- connaissances : entretiens avec le personnel (connaissent-ils le plan, le niveau de sécurité, la procédure en cas d'incident ?) ;
- équipements : état des véhicules, communications, trousses, réserves d'hibernation ;
- équité : mesures réelles pour le personnel national et les partenaires.

Exemple d'échantillon. L'auditeur interroge 30 employés : 27 connaissent le niveau de sécurité actuel (90 %), 18 savent quoi faire si un collègue ne répond pas à un contrôle d'appel (60 %), 9 ont participé à un exercice dans l'année (30 %). Les procédures écrites existent, mais leur appropriation est faible : formation et exercices deviennent prioritaires.

La culture de sécurité

Les procédures les mieux écrites échouent sans une **culture de sécurité** : un ensemble de comportements partagés où la sécurité est vue comme un moyen de faire le travail, pas comme un obstacle.

Ses signes :

- les incidents et les quasi-incidents sont signalés, et les erreurs discutées sans peur ;
- les responsables appliquent les règles qu'ils imposent ;
- chacun peut dire « non » ou « stop » sans être moqué ni sanctionné ;
- les personnels nationaux participent aux analyses et aux décisions ;
- la sécurité est discutée dans les réunions de programme, pas seulement entre spécialistes ;
- la qualité des programmes et le comportement personnel sont reconnus comme des mesures de sécurité.

> La culture se voit à ce qui se passe quand un responsable pressé veut contourner une règle. Si personne n'ose rien dire, la culture de sécurité est faible.

La continuité d'activité

Le **plan de continuité d'activité** prépare l'organisation à maintenir ses fonctions essentielles malgré une perturbation majeure : perte d'un bureau, coupure prolongée d'Internet, cyberattaque, pandémie, évacuation, départ brutal de personnes clés.

Étapes :

- **Identifier les fonctions critiques** : paiement des salaires, des fournisseurs et des transferts aux bénéficiaires, approvisionnement des centres de santé, communications avec les équipes, rapports aux bailleurs à échéance.
- **Fixer pour chacune un délai maximal d'interruption** : par exemple 24 heures pour les communications d'urgence, 7 jours pour la paie, 30 jours pour les rapports aux bailleurs.
- **Prévoir les solutions de repli** : bureau alternatif, accès à distance, sauvegardes, délégations de signature, fournisseurs de secours, stocks.
- **Désigner des suppléants** pour les fonctions clés et documenter les accès essentiels (sans partager de mots de passe en clair).
- **Tester** le plan au moins une fois par an.

Exemple. Le système de paie est hébergé sur un serveur au bureau de la capitale. Délai maximal toléré : 7 jours. Si le bureau devient inaccessible, la restauration à partir de la sauvegarde hors site prend 3 jours, ce qui respecte le délai, à condition que la sauvegarde soit récente et testée : la dernière date de 5 semaines. Action : sauvegarde quotidienne automatisée, test trimestriel de restauration.

Projet final : un cadre de gestion des risques pour un pays

Le projet final du Mini MBA Sécurité et gestion des risques consiste à rédiger, pour un pays ou une zone réels (avec des données publiques uniquement, jamais d'informations confidentielles d'une organisation) ou fictifs mais réalistes, un **cadre de gestion des risques** de 6 à 10 pages :

- **1. Analyse du contexte** : acteurs, dynamiques, scénarios, indicateurs.
- **2. Évaluation des risques** : menaces, vulnérabilités par profil, matrice, risques inhérents et résiduels, comparaison au seuil.
- **3. Stratégie** : dosage acceptation, protection, dissuasion, et stratégie d'accès et de négociation.
- **4. Plan de sécurité résumé** : niveaux, procédures clés, communications, plans de contingence (évacuation médicale, hibernation, relocalisation, enlèvement).
- **5. Personnes** : devoir de protection équitable, santé, bien-être, sauvegarde interne, assurances.
- **6. Risques de l'organisation** : extrait du registre (fiduciaire, conformité, PSEA, numérique, réputation).
- **7. Partenaires, budget et gouvernance** : partage du risque, budget de sécurité, tableau de bord, continuité d'activité.

Critères d'évaluation : qualité de l'analyse, cohérence entre risques et mesures, réalisme et proportionnalité, équité entre personnels et partenaires, respect des principes humanitaires, clarté. Le projet fait partie de l'examen du troisième mois.

Exercice d'application : préparer le rapport annuel au conseil

Situation. Données de l'année : 9 pays ; 210 incidents pour 1 400 employés (année précédente : 168 pour 1 200) ; incidents graves : 21 (année précédente : 12) ; plans à jour dans 7 pays ; exercices de crise dans 4 pays ; 2 pays avec un risque résiduel au-dessus de l'appétit ; 38 recommandations d'incidents, dont 22 mises en œuvre dans les délais ; plan de continuité testé : aucun. Les partenaires locaux ont signalé 35 incidents, mais ne sont pas inclus dans les statistiques officielles.

Travail demandé. 1) Calculez les taux et les pourcentages clés. 2) Que doit retenir le conseil ? 3) Quelles décisions lui demander ?

Corrigé. 1) Taux d'incidents : 15 pour 100 employés contre 14 l'an passé (+7 %). Taux d'incidents graves : 1,5 contre 1,0 pour 100 employés (+50 %). Plans à jour : 7 / 9 = 78 % ; exercices : 4 / 9 = 44 % ; recommandations dans les délais : 22 / 38 = 58 %. 2) La gravité augmente nettement plus que la fréquence ; la préparation est insuffisante (plans, exercices, continuité jamais testée) ; l'apprentissage est lent ; deux pays sont hors appétit ; les risques des partenaires sont invisibles dans les rapports. 3) Décisions : pour les 2 pays hors appétit, choisir entre mesures supplémentaires, réduction d'activités ou acceptation motivée et temporaire ; exiger des plans à jour et un exercice de crise dans tous les pays d'ici 6 mois ; tester le plan de continuité dans l'année ; intégrer les incidents des partenaires dans les rapports et budgéter leur sécurité ; suivre trimestriellement les recommandations en retard.

À retenir

- Une politique adoptée par le conseil, déclinée en normes minimales par niveau de risque.
- Le conseil porte la responsabilité ultime : appétit, rapports, information immédiate des crises, ressources.
- Auditer les documents, les pratiques, les connaissances, les équipements et l'équité.
- Culture de sécurité : signaler sans peur, pouvoir dire stop, exemplarité des responsables.
- Continuité d'activité : fonctions critiques, délais maximaux, solutions de repli, suppléants, tests réguliers.

Quiz

1. 9 pays, 6 avec un plan à jour. Pourcentage :
   A. 67 %
   B. 60 %
   C. 75 %
   D. 54 %
2. Incidents graves : 18 pour 1 200 employés. Taux pour 100 employés :
   A. 18
   B. 15
   C. 0,15
   D. 1,5
3. Lors d'un audit, 12 employés sur 40 savent quoi faire si un contrôle d'appel manque. Cela indique :
   A. Une bonne appropriation
   B. Un problème de radio
   C. Une faible appropriation (30 %) : formation et exercices prioritaires
   D. Rien de particulier
4. Dans un plan de continuité, le délai maximal d'interruption sert à :
   A. Calculer les salaires
   B. Dimensionner les solutions de repli de chaque fonction critique
   C. Évaluer le personnel
   D. Fixer le budget de communication
5. Un signe fort d'une bonne culture de sécurité est :
   A. Chacun peut dire « stop » sans être sanctionné
   B. Aucun incident signalé
   C. Des procédures très longues
   D. Des gardes armés

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