ACADÉMIE HUMANITAIRE · HUMANITAIRES JOBS

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

Manuel complet

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/

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

Sommaire

1. Semaine 1 : Devoir de protection et gestion des risques de sécurité : le cadre
2. Semaine 2 : Analyser le contexte : acteurs, dynamiques et tendances de la violence
3. Semaine 3 : Évaluer les risques : menaces, vulnérabilités, probabilité et impact
4. Semaine 4 : Plans de sécurité, procédures, déplacements et communications
5. Semaine 5 : Construire l'acceptation et négocier l'accès
6. Semaine 6 : Incidents : signaler, analyser, apprendre
7. Semaine 7 : Gérer une crise : cellule de crise, hibernation, relocalisation, évacuation, enlèvement
8. Semaine 8 : Santé, bien-être psychosocial, sauvegarde interne et assurances
9. Semaine 9 : Sécurité numérique et protection de l'information
10. Semaine 10 : Gérer tous les risques de l'organisation : registre, appétit, conformité et réputation
11. Semaine 11 : Partager le risque avec les partenaires et financer la sécurité
12. Semaine 12 : Gouvernance, culture de sécurité, continuité d'activité et projet final

Semaine 1 : Devoir de protection et gestion des risques de sécurité : le cadre

Objectifs

- Expliquer le devoir de protection (duty of care) d'une organisation humanitaire et ses conséquences juridiques, éthiques et opérationnelles.
- Décrire le cycle de gestion des risques de sécurité et les trois stratégies : acceptation, protection, dissuasion.
- Situer la sécurité au service de l'accès et des programmes : rester et agir, plutôt que fuir ou s'exposer.

Pourquoi la sécurité est une fonction de direction

Chaque année, des centaines de travailleurs humanitaires sont tués, blessés ou enlevés ; la grande majorité sont des **personnels nationaux**. Les bases de données publiques sur la sécurité des humanitaires montrent que les violences se concentrent dans un petit nombre de contextes, mais qu'aucune organisation travaillant en zone de crise n'est à l'abri.

La sécurité n'est pas d'abord une affaire de gardes et de murs. C'est une **fonction de direction** qui permet d'atteindre les personnes dans le besoin en gardant les risques pour le personnel à un niveau acceptable. Une organisation qui gère mal ses risques perd son accès, ses équipes, ses financements et parfois sa réputation.

> Objectif de la gestion des risques de sécurité : permettre un accès durable aux populations, pas éliminer tout risque. Le seul moyen d'éliminer tout risque est de ne rien faire.

Le devoir de protection

Le **devoir de protection** (duty of care) est l'obligation, juridique et morale, d'une organisation de prendre toutes les mesures raisonnables pour protéger son personnel contre les dommages prévisibles. Il s'étend, à des degrés divers, aux consultants, aux volontaires, aux visiteurs et aux partenaires.

En pratique, il exige :

- d'**évaluer** les risques avant d'exposer quelqu'un ;
- d'**informer** clairement le personnel des risques (consentement éclairé) ;
- de **former** et d'équiper ;
- de mettre en place des **mesures** proportionnées (procédures, communications, assurances, soutien psychosocial) ;
- de **répondre** aux incidents et d'apprendre.

Des décisions de justice dans plusieurs pays ont reconnu la responsabilité d'organisations humanitaires qui n'avaient pas pris de mesures raisonnables face à un risque connu. Le devoir de protection ne peut pas être délégué entièrement : une organisation reste responsable même quand elle s'appuie sur un prestataire ou sur un dispositif commun.

Il doit être **équitable** : historiquement, le personnel national a reçu moins de formation, d'équipement et d'options d'évacuation que le personnel international pour un risque égal ou plus élevé. Les bonnes pratiques actuelles exigent de traiter cette inégalité de façon explicite.

Le cycle de gestion des risques de sécurité

Le cadre le plus utilisé dans le secteur (formalisé notamment par la revue de bonnes pratiques n° 8 du Humanitarian Practice Network et les guides du Global Interagency Security Forum, GISF) suit un cycle :

- **1. Analyse du contexte** : acteurs, dynamiques, tendances de la violence.
- **2. Évaluation des risques** : menaces, vulnérabilités, probabilité, impact.
- **3. Choix des stratégies et des mesures** : acceptation, protection, dissuasion.
- **4. Plans et procédures** : plan de sécurité, procédures opérationnelles, plans de contingence.
- **5. Mise en œuvre** : formation, équipement, budget, responsabilités.
- **6. Suivi, incidents et révision** : signalement, analyse, mise à jour régulière.

Le cycle tourne en continu : toute évolution significative du contexte (élections, offensive militaire, incident grave) déclenche une révision, sans attendre la date prévue.

Acceptation, protection, dissuasion

Trois stratégies se combinent, avec un dosage propre à chaque contexte :

- **Acceptation** : obtenir le consentement des communautés, des autorités et des parties au conflit à la présence et aux activités de l'organisation, par la pertinence des programmes, le respect des principes, le dialogue et le comportement du personnel. C'est la stratégie de base des humanitaires.
- **Protection** : réduire la vulnérabilité par des mesures et des équipements (procédures de déplacement, murs, gardes non armés, communications, véhicules adaptés, abris). Elle protège mais peut éloigner l'organisation des communautés (« bunkerisation »).
- **Dissuasion** : opposer une menace pour dissuader une agression (gardes armés, escortes armées, suspension conditionnelle des activités). Elle est réservée aux cas exceptionnels car elle peut compromettre la neutralité et l'acceptation.

Exemple. Dans une zone où l'organisation est bien acceptée mais où la criminalité urbaine est forte, la combinaison typique est : acceptation dans les communautés d'intervention, protection renforcée des résidences et des déplacements en ville (pas de marche de nuit, véhicules verrouillés), et suspension des activités comme levier de dissuasion en cas d'attaque ciblée.

Le seuil de risque acceptable et le programme critique

Toute exposition doit être **justifiée par la valeur du programme**. Plus le risque est élevé, plus l'activité doit être critique pour les personnes (sauver des vies) et plus l'organisation doit avoir réellement les moyens de le gérer.

Les outils de **criticité des programmes** (par exemple le cadre des Nations unies) classent les activités de la plus critique (activité vitale immédiate, ou ordonnée par le Secrétaire général) à la moins critique. Une activité peu critique ne justifie pas un risque élevé ; une activité vitale peut justifier un risque élevé, mais pas un risque inacceptable.

Exemple de décision. Une formation en gestion de projet de trois jours, dans une ville où le risque d'enlèvement est jugé élevé, peut être déplacée ou faite en ligne. Une campagne de vaccination contre une épidémie dans la même ville peut être maintenue avec des mesures renforcées, parce que le bénéfice vital justifie un risque résiduel plus élevé, dans la limite fixée par la direction.

> Le seuil de risque acceptable est fixé par la direction de l'organisation, par écrit, et non par l'équipe la plus courageuse sur le terrain.

Les rôles et responsabilités

La sécurité est l'affaire de tous, mais les responsabilités doivent être claires :

- **Conseil d'administration et direction générale** : politique de sécurité, seuil de risque acceptable, ressources, supervision des incidents graves.
- **Directeur pays** : responsable de la sécurité dans le pays ; c'est un rôle de direction qui ne se délègue pas entièrement au conseiller sécurité.
- **Responsable ou conseiller sécurité** : analyse, conseil, procédures, formation, suivi des incidents.
- **Points focaux sécurité** dans les bases de terrain.
- **Chaque membre du personnel** : respecter les procédures, signaler, adopter un comportement qui protège l'acceptation, et dire non à une mission jugée trop dangereuse.

Le **droit de retrait** : toute personne peut refuser de se rendre dans un lieu ou peut quitter un lieu si elle estime le risque trop élevé, sans sanction. À l'inverse, la direction peut interdire un déplacement même si la personne est volontaire.

Exercice d'application : un directeur pays face à une demande de mission

Situation. Un bailleur demande une visite de suivi d'un projet d'éducation dans un district où trois véhicules d'ONG ont été braqués le mois dernier. Le personnel national de la base demande pourquoi les internationaux ont un gilet de protection et une option d'évacuation par avion, alors qu'eux n'ont ni assurance adaptée ni formation. Un jeune coordinateur international se porte volontaire pour la visite « parce qu'il n'a pas peur ».

Travail demandé. 1) Le niveau de risque est-il justifié par la criticité de l'activité ? 2) Quels problèmes de devoir de protection voyez-vous ? 3) Quelle décision et quelles mesures ?

Corrigé. 1) Une visite de suivi d'un projet d'éducation n'est pas une activité vitale : elle ne justifie pas un risque élevé. On cherche des alternatives : suivi à distance (appels, photos géolocalisées, partenaire local), vérification par un tiers mieux accepté, report, ou rencontre dans un lieu plus sûr. 2) Inégalité de traitement entre personnels nationaux et internationaux (assurance, formation, équipement, options de relocalisation) ; décision laissée au volontariat individuel au lieu d'une évaluation des risques et d'une décision de la direction. 3) Refuser la mission sous cette forme et expliquer au bailleur la solution de suivi alternative ; lancer une révision des mesures pour le personnel national (formation, assurance, plan de relocalisation pour ceux qui sont exposés du fait de leur emploi) ; rappeler que le seuil de risque est fixé par la direction et non par le volontariat.

À retenir

- La gestion des risques de sécurité sert l'accès aux populations ; elle ne vise pas le risque zéro.
- Devoir de protection : évaluer, informer, former, équiper, répondre et apprendre, de façon équitable entre personnels.
- Cycle : contexte, évaluation, stratégies, plans, mise en œuvre, suivi et révision.
- Acceptation d'abord ; protection selon les besoins ; dissuasion en dernier recours.
- Le risque acceptable dépend de la criticité du programme et est fixé par la direction, par écrit.

Quiz

1. La stratégie de sécurité de base des organisations humanitaires est :
   A. La dissuasion
   B. L'acceptation
   C. La protection
   D. L'évitement total

2. Le devoir de protection s'applique :
   A. À tout le personnel, et à des degrés divers aux consultants, volontaires et visiteurs
   B. Au personnel international seulement
   C. Seulement au personnel armé
   D. Uniquement en temps de guerre

3. Qui fixe le seuil de risque acceptable ?
   A. Les autorités locales
   B. Le membre du personnel le plus expérimenté
   C. Le bailleur
   D. La direction de l'organisation, par écrit

4. Des gardes armés autour d'un entrepôt relèvent de :
   A. L'acceptation
   B. La protection non armée
   C. La dissuasion
   D. L'évitement

5. Un membre du personnel refuse une mission qu'il juge trop dangereuse. Il :
   A. Doit être sanctionné
   B. Exerce son droit de retrait, sans sanction
   C. Doit démissionner
   D. Doit trouver un remplaçant

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

Semaine 2 : Analyser le contexte : acteurs, dynamiques et tendances de la violence

Objectifs

- Conduire une analyse de contexte structurée (politique, économique, sociale, sécuritaire) utile à la décision.
- Cartographier les acteurs selon leur influence, leurs intérêts et leur attitude envers l'organisation.
- Lire des données d'incidents (fréquences, taux, tendances) sans erreurs d'interprétation, et produire des indicateurs d'alerte.

Pourquoi analyser le contexte

Toutes les décisions de sécurité reposent sur une compréhension du contexte. Une analyse faible produit deux erreurs symétriques : **sous-estimer** une menace (et exposer le personnel) ou la **surestimer** (et abandonner des populations qui auraient pu être aidées).

Une bonne analyse répond à quelques questions : qui contrôle le territoire et les routes ? Quels sont les intérêts des acteurs, et comment l'action humanitaire les touche-t-elle ? Quels types de violence existent, contre qui, où, quand et pourquoi ? Qu'est-ce qui change ?

Sources : personnel national (la première source, souvent la plus fine), communautés, autorités, autres organisations, forums de coordination de la sécurité des ONG, Nations unies (UNDSS), médias locaux, réseaux sociaux (avec prudence), bases de données publiques de conflits. Toute information est **recoupée** et notée selon la fiabilité de la source et la crédibilité de l'information.

Les grilles d'analyse

Deux grilles simples structurent l'analyse :

- **PESTEL adapté** : politique, économique, social, technologique, environnemental, légal, auxquels on ajoute le sécuritaire (groupes armés, criminalité, forces de sécurité).
- **Analyse historique** : ligne du temps des événements majeurs des dernières années, pour repérer les cycles (saisons de combats, périodes électorales, récoltes, transhumance).

L'analyse aboutit à des **scénarios** : le plus probable, le plus dangereux, et éventuellement un scénario d'amélioration, chacun avec des **indicateurs** observables qui signalent qu'on s'en approche.

Exemple d'indicateurs. Scénario « reprise des combats autour de la ville » : déplacement de familles vers le sud, fermeture des marchés hebdomadaires, hausse soudaine du prix du carburant, départ des commerçants étrangers, mouvements de troupes signalés, discours hostiles sur les radios locales. Trois indicateurs sur six observés déclenchent une réunion de crise et la révision du niveau de sécurité.

Cartographier les acteurs

La **cartographie des acteurs** recense ceux qui peuvent influencer la sécurité et l'accès : autorités nationales et locales, forces armées et de police, groupes armés non étatiques, leaders traditionnels et religieux, milices, réseaux criminels, commerçants, médias, communautés d'accueil et déplacées, autres organisations.

Pour chacun : **influence** (faible à forte), **attitude** envers l'organisation (hostile, neutre, favorable), **intérêts** et **relation** actuelle.

Acteur	Influence	Attitude	Action
Chef de la principale milice	Forte	Neutre, méfiante	Dialogue régulier par un intermédiaire accepté ; expliquer les principes et les critères de ciblage
Préfet	Forte	Favorable	Information régulière, respect des procédures administratives
Jeunes sans emploi de la ville	Moyenne	Hostile (recrutements jugés injustes)	Transparence des recrutements, mécanisme de plainte, emplois journaliers équitables

> Un acteur hostile à forte influence est une priorité de l'analyse et de la stratégie d'acceptation, pas seulement une menace à éviter.

Lire les données d'incidents

Les données d'incidents aident à objectiver la menace, à condition de les lire correctement :

- **Fréquence brute** : nombre d'incidents par période.
- **Taux** : incidents rapportés à l'exposition (nombre d'employés, de déplacements, de jours-personne). Sans dénominateur, une hausse peut simplement refléter une augmentation de l'activité.
- **Biais de signalement** : une hausse peut venir d'un meilleur signalement, pas d'une aggravation.
- **Typologie** : un même total peut cacher une baisse des vols et une hausse des enlèvements, bien plus graves.

Exemple. Année 1 : 24 incidents pour 300 employés. Année 2 : 36 incidents pour 600 employés. Taux : 8 contre 6 incidents pour 100 employés par an. Malgré une hausse brute de 50 %, le taux a baissé de 25 %. Mais si les incidents graves (violences contre les personnes) passent de 3 à 9, leur taux passe de 1 à 1,5 pour 100 employés : la gravité augmente. La lecture combine taux et gravité.

Comprendre la violence contre les humanitaires

Les attaques contre les humanitaires ont plusieurs logiques, qu'il faut distinguer car elles appellent des réponses différentes :

- **Criminelle** : gain financier (vols, braquages, enlèvements contre rançon). Les mesures de protection et la discrétion sur les biens de valeur sont efficaces.
- **Politique ou militaire** : l'organisation est perçue comme alliée d'un camp, ou son action dérange une stratégie. L'acceptation, la neutralité perçue et la communication sont centrales.
- **Liée au travail lui-même** : conflits de ciblage, recrutements contestés, licenciements, plaintes non traitées. La qualité et la redevabilité des programmes sont des mesures de sécurité.
- **Incidentelle** : se trouver au mauvais endroit au mauvais moment (tirs croisés, bombardements, mines). Analyse des zones et des horaires, procédures de mouvement.

Beaucoup d'incidents graves touchant des ONG sont liés à des **tensions internes ou de voisinage** (personnel licencié, fournisseur écarté, bénéficiaire exclu) : l'analyse de sécurité doit regarder aussi l'organisation elle-même.

Produire une analyse utile

Une analyse utile tient en **deux pages**, est mise à jour régulièrement (mensuellement en contexte instable, après tout événement majeur), et se termine par des implications concrètes :

- zones et routes accessibles, sous conditions, ou interdites ;
- horaires et modes de déplacement ;
- acteurs à rencontrer et messages clés ;
- indicateurs à surveiller et seuils de révision ;
- conséquences pour les programmes (calendrier, modalités, gestion à distance).

Elle est partagée avec les personnes qui en ont besoin, en respectant la **confidentialité** : une analyse qui nomme des acteurs armés ou des informateurs peut mettre des personnes en danger si elle circule. Elle ne doit pas non plus utiliser d'informations confidentielles provenant d'autres organisations sans leur accord explicite.

Exercice d'application : une ville qui change

Situation. Une ONG travaille depuis 3 ans dans une ville de garnison. Données : année 1, 18 incidents pour 150 employés (dont 2 contre les personnes) ; année 2, 27 incidents pour 300 employés (dont 6 contre les personnes). Depuis un mois : un candidat local non recruté menace publiquement l'organisation ; deux marchés hebdomadaires sont fermés ; les loyers baissent car des familles aisées partent ; une radio locale accuse « les ONG » d'aider les rebelles ; le forum de sécurité des ONG signale des mouvements de troupes.

Travail demandé. 1) Calculez et interprétez les taux d'incidents. 2) Classez les signaux par logique de violence. 3) Proposez trois implications pratiques.

Corrigé. 1) Taux global : 12 puis 9 incidents pour 100 employés (baisse de 25 %). Taux d'incidents contre les personnes : 1,33 puis 2 pour 100 employés (hausse de 50 %). La situation s'aggrave en gravité malgré la baisse du taux global. 2) Menace du candidat non recruté : logique liée au travail ; accusations radiophoniques : logique politique (perception de partialité) ; marchés fermés, départs, mouvements de troupes : indicateurs d'un scénario de reprise des combats (risque incidentel et politique). 3) Traiter la plainte de recrutement (mécanisme formel, transparence, sécurité du personnel des RH) ; lancer une démarche d'acceptation (rencontres avec les autorités et leaders, émission de radio sur les principes et les critères d'aide) ; réviser le scénario et le niveau de sécurité, préparer la relocalisation et la gestion à distance si les indicateurs militaires se confirment.

À retenir

- Une analyse faible sous-estime ou surestime ; recouper et noter fiabilité et crédibilité des sources.
- Scénarios avec indicateurs observables et seuils qui déclenchent une révision.
- Cartographier influence, attitude et intérêts des acteurs ; prioriser les acteurs hostiles influents.
- Toujours un dénominateur : taux d'incidents par exposition, lus avec la gravité.
- Beaucoup d'incidents graves ont une origine liée au travail : la qualité des programmes est une mesure de sécurité.

Quiz

1. 30 incidents pour 500 employés. Le taux pour 100 employés est :
   A. 30
   B. 16,7
   C. 6
   D. 0,6

2. Les incidents passent de 20 à 30 pendant que le personnel passe de 200 à 400. Le taux :
   A. Augmente de 50 %
   B. Baisse de 25 %
   C. Reste stable
   D. Double

3. Un licenciement mal géré suivi de menaces relève surtout d'une violence :
   A. Liée au travail de l'organisation
   B. Incidentelle
   C. Criminelle
   D. Militaire

4. Une analyse de sécurité qui nomme des informateurs doit :
   A. Être publiée pour la transparence
   B. Être partagée avec tous les partenaires
   C. Être envoyée aux médias
   D. Circuler de façon strictement restreinte pour ne pas les mettre en danger

5. Un acteur hostile et très influent doit être :
   A. Ignoré
   B. Signalé à la presse
   C. Une priorité de l'analyse et de la stratégie d'acceptation
   D. Contourné sans jamais être contacté

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

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

Semaine 4 : Plans de sécurité, procédures, déplacements et communications

Objectifs

- Rédiger un plan de sécurité de pays ou de zone, avec des niveaux de sécurité et des mesures associées.
- Concevoir des procédures opérationnelles standard réalistes, en particulier pour les déplacements et les sites.
- Mettre en place un système de communications et de suivi des mouvements qui fonctionne quand tout le reste tombe.

Le plan de sécurité

Le **plan de sécurité** traduit l'évaluation des risques en règles et en responsabilités. Il est court, pratique, connu de tous et révisé régulièrement. Contenu type :

- résumé du contexte et des principales menaces ;
- stratégie (dosage acceptation, protection, dissuasion) ;
- niveaux de sécurité et mesures associées ;
- procédures opérationnelles standard (déplacements, sites, communications, visiteurs, argent liquide, incidents) ;
- plans de contingence (évacuation médicale, hibernation, relocalisation, évacuation, enlèvement, attaque) ;
- organigramme de sécurité et contacts d'urgence ;
- annexes : cartes, listes de personnel, inventaire des équipements de communication.

Chaque nouvel arrivant reçoit un **briefing de sécurité** à l'arrivée et signe qu'il a lu le plan. Un plan de 80 pages que personne n'a lu ne protège personne.

Les niveaux de sécurité

La plupart des organisations utilisent 4 ou 5 **niveaux de sécurité** par zone, chacun associé à des mesures automatiques, ce qui accélère les décisions en période de tension :

Niveau	Situation	Mesures types
1. Normal	Risques faibles et stables	Procédures standard
2. Vigilance	Tensions, incidents isolés	Déplacements limités en horaires, contrôle d'appel renforcé, révision des plans
3. Restriction	Violence en hausse, menaces ciblées possibles	Déplacements essentiels seulement, sur autorisation ; réduction du personnel non essentiel ; activités adaptées
4. Hibernation ou relocalisation	Violence généralisée ou ciblée	Regroupement dans un lieu sûr, ou départ du personnel le plus exposé ; activités suspendues ou à distance
5. Évacuation et suspension	Risque inacceptable	Départ de la zone ou du pays selon le plan ; maintien du contact avec le personnel resté

Le passage d'un niveau à l'autre est décidé par le directeur pays, sur la base d'**indicateurs** définis à l'avance (voir semaine 2), et communiqué immédiatement à tous.

Les procédures de déplacement

Les déplacements sont le moment où le personnel est le plus exposé. Procédure type :

- **Autorisation** préalable selon le niveau de sécurité, sur la base d'un plan de déplacement : itinéraire, horaires, passagers, véhicules, contacts.
- **Vérification de la route** le matin même : forum de sécurité, autorités, transporteurs, personnel local.
- **Véhicule** vérifié et équipé : carburant, roue de secours, trousse, communications.
- **Contrôle d'appel** (check-in) à intervalles fixés et à chaque point clé ; procédure claire si un appel manque.
- **Couvre-feu interne** : arrivée avant une heure fixée, avec marge.
- **Comportement** aux points de contrôle et en cas de braquage (pas de résistance, pas de photos, calme, coopération).

Calcul de départ. Trajet de 180 km, vitesse moyenne réaliste 40 km/h : 4 h 30. Couvre-feu interne 17 h, marge d'une heure : arrivée prévue au plus tard à 16 h. Départ au plus tard à 11 h 30. Avec un contrôle d'appel toutes les heures et à l'arrivée : 5 appels. Si un appel manque, la base tente un nouveau contact pendant 15 minutes, puis déclenche la procédure de véhicule manquant.

Sécurité des sites

Bureaux, résidences, entrepôts et sites de distribution font l'objet d'une évaluation et de mesures adaptées :

- **Choix du site** : quartier, voisinage (éviter la proximité de cibles potentielles : bâtiments militaires, ministères sensibles), deux voies d'accès, distance des zones à risque

d'inondation.

- **Périmètre** : mur ou clôture, portail, éclairage, gardes non armés formés, contrôle des visiteurs.
- **Bâtiment** : portes et fenêtres solides, pièce sûre ou abri selon les menaces (pièce renforcée contre les intrusions, abri contre les tirs indirects).
- **Sécurité incendie et électrique** : extincteurs, détecteurs, issues de secours.
- **Réserves** : eau, nourriture, carburant, médicaments pour l'hibernation (souvent 7 à 14 jours).

Calcul de réserves. 12 personnes, hibernation de 10 jours : eau à 4 litres par personne et par jour pour la boisson et un usage minimal = 480 litres ; avec 20 % de marge, environ 580 litres. Nourriture : 12 × 10 = 120 rations journalières. Carburant pour un générateur à 2 litres par heure, 8 heures par jour : 160 litres.

Les communications

Le système de communications doit fonctionner **quand le réseau mobile est coupé**, ce qui arrive souvent au moment où l'on en a le plus besoin. Principe de redondance : au moins deux moyens indépendants.

- **Téléphone mobile** : pratique, mais fragile et surveillable.
- **Radio HF** : longue distance, indépendante des réseaux, mais nécessite des opérateurs formés et des licences.
- **Radio VHF** : courte portée, idéale en ville et en convoi, avec relais.
- **Téléphone satellitaire** et terminaux satellitaires de données : indépendants, mais coûteux et parfois réglementés ou mal perçus par les autorités.
- **Balises de suivi** GPS avec bouton d'alerte.

Règles : indicatifs d'appel, langage clair mais sans informations sensibles (pas de noms, de montants d'argent ou d'itinéraires détaillés à la radio), arbre d'appel (chaque responsable appelle un nombre défini de personnes), tests réguliers, chargeurs et batteries de secours. Les communications sont aussi un sujet d'acceptation : utiliser une radio ou un téléphone satellitaire là où les autorités l'interdisent peut faire soupçonner d'espionnage.

Des procédures qui sont réellement appliquées

Les procédures échouent souvent pour des raisons simples : trop nombreuses, mal connues, impossibles à appliquer, ou contournées par habitude. Bonnes pratiques :

- Écrire **peu** de procédures, courtes, adaptées au contexte réel, avec le personnel qui les appliquera.
- Les **expliquer** (le pourquoi) et pas seulement les imposer.
- Les **exercer** : simulations de véhicule manquant, d'hibernation, d'évacuation médicale, au moins deux fois par an.
- Les **vérifier** : contrôles ponctuels des carnets de bord, des contrôles d'appel, des registres de visiteurs.

- Traiter le non-respect comme un sujet de **management** : un responsable qui contourne les procédures donne l'exemple à toute l'équipe.

> La complaisance est un risque à part entière : après des mois sans incident, les procédures se relâchent précisément au moment où le contexte peut basculer.

Exercice d'application : planifier une mission de terrain

Situation. Une équipe de 4 personnes doit se rendre de la base à un site à 210 km pour une distribution. Vitesse moyenne réaliste : 35 km/h. Couvre-feu interne : 17 h 30, avec une marge d'une heure. La distribution dure 3 heures. Le site n'a pas de réseau mobile sur les 80 derniers kilomètres. Le niveau de sécurité de la zone est « vigilance ». Le chauffeur propose de partir à 9 h « comme d'habitude ».

Travail demandé. 1) La mission peut-elle se faire aller-retour dans la journée ? 2) Sinon, quelle organisation ? 3) Quels moyens de communication et quels contrôles d'appel ?

Corrigé. 1) Trajet : 210 / 35 = 6 heures. Aller-retour 12 heures + 3 heures de distribution = 15 heures ; arrivée au plus tard à 16 h 30 : départ à 1 h 30 du matin, impossible (pas de circulation de nuit). La mission ne peut pas se faire dans la journée. 2) Nuit sur place ou dans une ville étape sûre, dans un hébergement évalué à l'avance ; ou découper : jour 1 trajet (départ à 9 h, arrivée vers 15 h), jour 2 distribution et retour partiel, ou distribution par un partenaire local avec suivi. Varier l'heure de départ habituelle, qui rend les mouvements prévisibles. 3) Téléphone mobile là où le réseau existe, téléphone satellitaire ou radio HF pour les 80 km sans réseau, balise de suivi ; contrôle d'appel toutes les heures et à chaque point clé (départ, entrée dans la zone sans réseau, arrivée, début et fin de distribution) ; procédure de véhicule manquant connue de la base.

À retenir

- Un plan de sécurité court, connu, signé à l'arrivée, révisé régulièrement.
- Niveaux de sécurité avec mesures automatiques et indicateurs de passage définis à l'avance.
- Déplacements : autorisation, vérification de la route, contrôle d'appel, couvre-feu avec marge, non-résistance.
- Communications redondantes, testées, sans informations sensibles en clair.
- Peu de procédures, expliquées, exercées, vérifiées ; la complaisance est un risque.

Quiz

1. Trajet de 160 km à 40 km/h, arrivée au plus tard à 16 h. Départ au plus tard :
   A. 12 h
   B. 10 h
   C. 14 h
   D. 11 h

2. 10 personnes, 7 jours d'hibernation, 4 litres d'eau par personne et par jour. Eau minimale :
   A. 70 litres
   B. 400 litres
   C. 40 litres
   D. 280 litres

3. Pourquoi exiger deux moyens de communication indépendants ?
   A. Pour réduire les coûts
   B. Parce que les bailleurs l'exigent
   C. Parce que le réseau mobile tombe souvent au moment critique
   D. Pour communiquer avec la presse

4. À la radio, on évite de mentionner :
   A. Les indicatifs d'appel
   B. Les noms, montants d'argent et itinéraires détaillés
   C. L'heure
   D. Le niveau de sécurité

5. Après six mois sans incident, l'équipe relâche les contrôles d'appel. C'est :
   A. De la complaisance, un risque à corriger par le management
   B. Normal et sans risque
   C. Une bonne adaptation
   D. Une décision du chauffeur

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

Semaine 5 : Construire l'acceptation et négocier l'accès

Objectifs

- Construire une stratégie d'acceptation fondée sur les principes, la qualité des programmes et le dialogue avec tous les acteurs.
- Mesurer l'acceptation avec des indicateurs concrets plutôt que de la supposer.
- Préparer et conduire une négociation d'accès humanitaire avec un acteur armé, en fixant ses lignes rouges.

L'acceptation n'est pas un acquis

L'**acceptation** est le consentement, actif ou passif, des acteurs qui peuvent nuire à l'organisation. Elle ne se décrète pas : elle se construit et s'entretient, et elle peut se perdre en une journée.

Elle repose sur plusieurs piliers :

- **Les principes** : humanité, neutralité, impartialité, indépendance, compris et perçus comme réels.
- **La qualité et la pertinence** des programmes : une aide utile, juste et bien ciblée.
- **La redevabilité** : les communautés savent ce qu'elles peuvent attendre et peuvent se plaindre.
- **Le comportement** du personnel : respect, discrétion, absence d'arrogance, pas d'exploitation ni d'abus.
- **Le dialogue** avec tous les acteurs qui ont une influence, y compris les groupes armés non étatiques.
- **La cohérence** : mêmes critères partout, même discours à tous.

L'acceptation est souvent **locale et personnelle** : elle tient à une équipe, à un responsable respecté. Elle ne se transfère pas automatiquement d'une zone à une autre ni d'une personne à une autre.

Ce qui détruit l'acceptation

Les pertes d'acceptation viennent souvent de l'organisation elle-même :

- Ciblage perçu comme injuste ou capté par une élite ou un groupe.
- Recrutements perçus comme favorisant un clan ou excluant la population locale.
- Promesses non tenues, programmes interrompus sans explication.
- Association visible avec une partie au conflit (escortes militaires, logos de forces armées, présence dans des réunions militaires médiatisées).

- Comportement personnel : conduite dangereuse, consommation d'alcool ostentatoire dans un contexte conservateur, relations jugées inappropriées.
- Communication publique imprudente : un communiqué au siège ou un message sur les réseaux sociaux lu localement comme une prise de position.

> Un tweet du siège peut annuler des mois de travail d'acceptation sur le terrain : la communication externe fait partie de la gestion des risques.

Mesurer l'acceptation

L'acceptation se suppose trop souvent (« les gens nous aiment »). On peut la **mesurer** avec des indicateurs :

- Les communautés et leaders connaissent-ils l'organisation, ses activités et ses principes ? (enquêtes de perception, entretiens)
- L'organisation reçoit-elle des **alertes** spontanées (« ne passez pas par là demain ») ?
- Ses demandes d'accès sont-elles accordées, et dans quels délais ?
- Les plaintes reçues portent-elles sur la qualité de l'aide ou sur la présence de l'organisation elle-même ?
- Les incidents la ciblent-ils plus ou moins que d'autres organisations comparables ?

Exemple. Enquête de perception auprès de 300 personnes dans deux districts : district A, 78 % connaissent l'organisation et 70 % jugent l'aide « juste » ; district B, 41 % la connaissent et 35 % jugent l'aide « juste ». L'acceptation est nettement plus faible en B, où l'équipe se sentait pourtant « bien acceptée ». Actions : rencontres communautaires, diffusion des critères de ciblage, revue des listes avec les comités, recrutement local plus équilibré.

Négocier l'accès : préparation

La **négociation humanitaire** vise à obtenir l'accès aux populations, la sécurité des équipes et le respect des principes, dans un dialogue souvent asymétrique. Les méthodes structurées (par exemple celles du Centre de compétences en négociation humanitaire, CCHN) insistent sur la préparation :

- **Analyse de l'interlocuteur** : intérêts, motivations, normes, contraintes, réseau, qui il doit convaincre lui-même.
- **Analyse de son propre mandat** : ce qu'on peut offrir, ce qu'on ne peut pas.
- **Lignes rouges** fixées et validées à l'avance par la hiérarchie : pas de paiement, pas de détournement de l'aide, pas de liste de bénéficiaires imposée, pas d'escorte du groupe armé si elle compromet la neutralité.
- **Zone de négociation** : les points ouverts à l'échange (calendrier, modalités, communication, choix des sites).
- **Équipe** : qui négocie (personne acceptée, langue, profil), qui soutient, qui décide.
- **Plan B** : que fait-on en cas d'échec ? (meilleure alternative à un accord négocié)

Négocier l'accès : conduite et suivi

Principes de conduite :

- Commencer par établir la **relation** et la confiance ; écouter avant de demander.
- Parler des **besoins des populations** que l'interlocuteur dit défendre : beaucoup d'acteurs armés veulent être vus comme protégeant « leur » population.
- Expliquer les principes en termes concrets : impartialité = aide selon les besoins, pour tous ; neutralité = ne pas prendre parti, y compris contre lui.
- Ne jamais promettre ce qu'on ne peut pas tenir ; ne jamais céder sur une ligne rouge sous la pression : demander du temps et en référer.
- Garder la **trace** de ce qui est convenu, et informer les autres acteurs concernés si nécessaire, sans mettre personne en danger.

Suivi. Un accord d'accès se vérifie à l'usage : les équipes passent-elles réellement ? Les engagements sont-ils tenus des deux côtés ? Toute violation (taxation, détournement, menace) fait l'objet d'une analyse et d'une réponse proportionnée : rappel, suspension partielle, suspension totale, coordination avec les autres organisations pour éviter qu'un groupe ne joue les ONG les unes contre les autres.

Coordination et positions communes

Négocier seul expose l'organisation à des demandes qu'elle ne peut pas refuser sans risque, ou qu'une autre organisation acceptera. La **coordination** renforce la position de tous :

- **Règles opérationnelles communes** (ground rules) entre organisations d'une zone : pas de paiement aux points de contrôle, pas d'escortes armées sauf exception, refus collectif des listes imposées.
- **Groupes de travail sur l'accès** animés par OCHA, qui suivent les contraintes d'accès et portent un plaidoyer commun.
- **Forums de sécurité des ONG** qui partagent l'information et les analyses.

Limites : la coordination ne doit pas faire perdre l'**indépendance** de chaque organisation, ni l'associer à des positions politiques. Certaines organisations, comme le CICR, conduisent leurs propres négociations confidentielles. La coordination se fait sur des principes et des pratiques, pas sur un alignement aveugle.

Exercice d'application : un point de contrôle qui « taxe »

Situation. Un groupe armé contrôle la route vers 3 camps de déplacés (25 000 personnes). Depuis deux semaines, il exige 50 USD par camion d'aide et demande que 10 % des vivres soient « remis aux combattants qui protègent les camps ». Deux ONG ont commencé à payer « pour ne pas abandonner les gens ». Votre organisation distribue des vivres et gère un centre de santé. Une enquête de perception récente montre que 74 % des habitants des camps vous connaissent et jugent votre aide juste.

Travail demandé. 1) Quelles sont vos lignes rouges ? 2) Quels leviers et quels intérêts du groupe pouvez-vous mobiliser ? 3) Quel plan si la négociation échoue ?

Corrigé. 1) Aucun paiement ni part de l'aide à une partie au conflit (violation des principes, des règles des bailleurs et souvent des lois antiterroristes) ; pas de distribution sous contrôle du groupe ; liste de bénéficiaires établie par l'organisation selon les besoins. 2) Leviers : l'acceptation forte dans les camps (le groupe veut être vu comme protecteur des déplacés) ; l'importance du centre de santé, y compris pour les familles des combattants (soins impartiaux à tous) ; une position commune avec les autres organisations via le groupe de travail sur l'accès ; l'intervention de leaders religieux ou traditionnels respectés par le groupe. 3) Coordonner avec OCHA et les ONG pour que les paiements cessent collectivement ; si l'accès reste conditionné, suspendre temporairement les convois de vivres en expliquant pourquoi aux communautés et au groupe ; envisager des modalités alternatives (transferts monétaires si les marchés le permettent, achats locaux dans les camps) ; maintenir le centre de santé si son accès ne dépend pas des convois ; documenter et informer les bailleurs.

À retenir

- L'acceptation se construit, s'entretient, se mesure, et peut se perdre en un jour.
- Ciblage, recrutement, comportement et communication publique : premières causes de perte d'acceptation.
- Négocier : analyser l'interlocuteur, fixer les lignes rouges, connaître sa zone d'échange et son plan B.
- Aucun paiement ni part de l'aide à une partie au conflit : ligne rouge commune.
- Les règles communes entre organisations renforcent chacune, sans sacrifier l'indépendance.

Quiz

1. Quel signe indique une acceptation réelle ?
   A. Le personnel se sent bien
   B. La communauté donne des alertes spontanées sur les dangers
   C. Le bailleur est satisfait
   D. Les bureaux sont bien protégés

2. Une ligne rouge de négociation doit être :
   A. Fixée et validée à l'avance par la hiérarchie
   B. Improvisée pendant la réunion
   C. Négociable si l'interlocuteur insiste
   D. Secrète même pour l'équipe

3. Un groupe armé exige 5 % de l'aide. La réponse conforme aux principes :
   A. Accepter pour garder l'accès
   B. Payer en espèces plutôt qu'en vivres
   C. Accepter en secret
   D. Refuser, chercher une position commune et d'autres leviers, suspendre si nécessaire

4. Pourquoi coordonner des règles communes entre organisations ?
   A. Pour partager les budgets
   B. Pour supprimer l'indépendance de chacune
   C. Pour éviter qu'un acteur ne joue les organisations les unes contre les autres
   D. Pour éviter de parler aux communautés

5. Dans une enquête, 40 % des habitants connaissent l'organisation dans un district où l'équipe se croit bien acceptée. Conclusion :
   A. L'enquête est fausse
   B. L'acceptation est probablement surestimée ; renforcer l'information et le dialogue
   C. Il faut quitter le district
   D. Rien à faire

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

Semaine 6 : Incidents : signaler, analyser, apprendre

Objectifs

- Mettre en place un système de signalement des incidents et des quasi-incidents qui encourage la remontée d'information.
- Analyser un incident avec une méthode structurée (chronologie, causes, facteurs contributifs) sans culture de la faute.
- Exploiter les données d'incidents pour ajuster les mesures et rendre compte à la direction et aux bailleurs.

Pourquoi signaler

Un **incident de sécurité** est tout événement qui a causé ou aurait pu causer un dommage au personnel, aux biens, à la réputation ou aux programmes. Le **quasi-incident** (near miss) est un événement qui aurait pu causer un dommage mais n'en a pas causé : tirs entendus près d'un convoi, faux point de contrôle évité de justesse, menace verbale.

Signaler sert à :

- **porter assistance** immédiatement aux personnes touchées ;
- **alerter** les autres équipes et organisations ;
- **comprendre** les tendances et adapter les mesures ;
- **rendre compte** à la direction, au conseil, aux bailleurs et aux assureurs ;
- **prouver** que l'organisation exerce son devoir de protection.

La pyramide des incidents (observée dans de nombreux secteurs) montre qu'avant un incident grave, il y a généralement beaucoup de quasi-incidents et d'incidents mineurs. Ne pas les signaler, c'est se priver des alertes précoces.

Le système de signalement

Un système efficace comprend trois niveaux :

- **Alerte immédiate** (dans l'heure) : appel ou message à la personne désignée, avec les informations essentielles : qui, quoi, où, quand, état des personnes, besoin d'aide.
- **Rapport d'incident** (sous 24 à 48 heures) : formulaire standard avec chronologie, conséquences, actions prises.
- **Analyse** (sous 1 à 2 semaines pour les incidents significatifs) : causes, leçons, recommandations.

Pour encourager le signalement :

- formulaire simple, disponible hors ligne et dans les langues du personnel ;

- **pas de sanction** pour le signalement d'une erreur de bonne foi (culture « juste », qui distingue l'erreur honnête de la négligence grave ou de la violation délibérée) ;
- canal **confidentiel** pour les incidents sensibles (violences sexuelles, harcèlement, incidents impliquant un collègue) ;
- **retour d'information** : les équipes voient ce qui change grâce à leurs signalements.

> Si une équipe ne signale jamais rien, ce n'est presque jamais parce qu'il ne se passe rien. C'est un signal d'alerte sur la culture de sécurité.

Classer les incidents

Une **typologie** commune rend les données comparables : violence contre les personnes (meurtre, blessure, enlèvement, agression sexuelle, détention arbitraire), vol et braquage, intrusion, menace, incident lié au conflit (tirs, bombardements, engins explosifs), accident de la route, incident de santé, incident de sécurité numérique, troubles civils.

Chaque incident reçoit aussi un **niveau de gravité**, par exemple de 1 (mineur, sans blessé ni perte significative) à 4 (critique : décès, enlèvement, blessure grave, retrait d'une zone).

Exemple de tableau trimestriel. 42 incidents signalés : 15 vols mineurs, 9 menaces, 6 accidents de la route (dont 2 graves), 5 braquages de véhicules, 4 quasi-incidents liés aux combats, 2 détentions arbitraires de courte durée, 1 agression physique. Les incidents de gravité 3 et 4 sont au nombre de 8, soit 19 %. Les 5 braquages ont tous eu lieu sur le même axe, entre 15 h et 17 h : la tendance est exploitable (changement d'horaires, révision des autorisations sur cet axe).

Analyser un incident

L'analyse d'un incident significatif cherche à comprendre, pas à punir. Méthode en quatre temps :

- **Chronologie** précise, reconstituée à partir de plusieurs sources (personnes impliquées, témoins, communications, GPS).
- **Faits et conséquences** : dommages, réactions, assistance fournie.
- **Causes et facteurs contributifs** : contexte (menace), vulnérabilités (procédures, comportement, équipement), décisions prises et leurs raisons, ce qui a bien fonctionné.
- **Recommandations** : mesures concrètes, responsables, délais, et vérification de leur mise en œuvre.

Questions utiles : la menace était-elle connue ? Les procédures étaient-elles adaptées ? Étaient-elles connues et appliquées ? Si non, pourquoi (impossibles, inconnues, contournées) ? La réponse à l'incident a-t-elle été rapide et adaptée ? Qu'aurions-nous dû voir venir ?

Les personnes touchées doivent être **protégées** pendant l'analyse : soutien psychologique, respect du rythme, confidentialité, et pas d'interrogatoire répété qui les traumatise de nouveau.

Utiliser les données

Les données d'incidents alimentent :

- l'**analyse de contexte** et l'évaluation des risques (fréquences, lieux, horaires, auteurs, modes opératoires) ;
- les **décisions** sur les mesures (ce qui marche, ce qui ne marche pas) ;
- les **rapports** à la direction (tableau de bord trimestriel) et au conseil ;
- le **partage** avec les forums de sécurité et les bases de données sectorielles, de façon anonymisée et avec l'accord de l'organisation.

Indicateurs utiles. Nombre d'incidents pour 100 employés ; part des incidents graves ; délai moyen de signalement ; part des recommandations mises en œuvre dans les délais. **Exemple :** 24 recommandations issues des analyses de l'année ; 15 mises en œuvre dans les délais, 5 en retard, 4 non commencées. Taux de mise en œuvre dans les délais : 62,5 %. Les 4 non commencées sont examinées en priorité par la direction : une recommandation non appliquée laisse le risque intact.

Rendre compte et communiquer

Après un incident grave, plusieurs publics attendent des informations, avec des besoins différents :

- **Famille** des personnes touchées : information rapide, humaine, par une personne désignée, avant toute communication publique.
- **Personnel** : information factuelle, mesures prises, soutien disponible, pour éviter les rumeurs.
- **Bailleurs** : selon les contrats, notification rapide des incidents graves et de leurs conséquences sur les programmes.
- **Assureurs** : déclaration dans les délais pour les dommages et les frais médicaux.
- **Autres organisations** : alerte par le forum de sécurité.
- **Médias** : seulement par le porte-parole désigné ; dans le cas d'un enlèvement, la communication publique peut mettre la victime en danger et est décidée par la cellule de crise.

Une communication maladroite peut aggraver un incident : publier le nom d'une victime avant sa famille, accuser publiquement un acteur armé, ou révéler des informations qui compromettent une négociation.

Exercice d'application : analyser un braquage

Situation. Un véhicule de l'organisation a été braqué à 16 h 40 sur l'axe sud, à 25 km de la base ; le chauffeur et deux employés n'ont pas été blessés, mais le véhicule, deux ordinateurs et 4 000 USD de per diem en espèces ont été pris. Faits : l'autorisation de mouvement prévoyait une arrivée avant 16 h ; la distribution avait pris du retard ; le contrôle d'appel de 16 h n'a pas été fait (pas de réseau) ; le responsable de base n'a déclenché la procédure de véhicule manquant qu'à 17 h 30. Le trimestre précédent, 3 quasi-incidents avaient été signalés sur le même axe en fin d'après-midi, sans changement des procédures. Les per diem en espèces étaient transportés « pour simplifier ».

Travail demandé. 1) Facteurs contributifs. 2) Ce qui a bien fonctionné. 3) Recommandations.

Corrigé. 1) Départ tardif sans réévaluation (procédure de couvre-feu non appliquée face au retard) ; zone sans réseau sans moyen de communication alternatif ; délai de 90 minutes avant le déclenchement de la procédure de véhicule manquant ; quasi-incidents antérieurs non exploités ; transport d'argent liquide visible et non nécessaire. 2) Non-résistance du personnel, sans blessure ; signalement immédiat après l'incident. 3) Règle claire : en cas de retard, rester sur place dans un lieu sûr évalué à l'avance plutôt que rouler en fin d'après-midi sur cet axe ; téléphone satellitaire ou balise pour les zones sans réseau ; procédure de véhicule manquant déclenchée au plus tard 15 minutes après un appel manqué ; analyse systématique des quasi-incidents ; paiement des per diem par mobile money ou virement, et plafond de transport d'espèces ; soutien psychologique pour les trois employés ; responsables et délais pour chaque recommandation, suivi par le directeur pays.

À retenir

- Signaler incidents et quasi-incidents : la base de la pyramide prévient le sommet.
- Trois niveaux : alerte immédiate, rapport sous 48 heures, analyse des incidents significatifs.
- Culture juste : pas de sanction pour l'erreur honnête signalée ; canaux confidentiels.
- Analyser pour comprendre : chronologie, causes, facteurs contributifs, recommandations suivies.
- Après un incident grave : la famille d'abord, un porte-parole unique, prudence absolue en cas d'enlèvement.

Quiz

1. Des tirs entendus près d'un convoi, sans blessé ni dégât, constituent :
   A. Rien à signaler
   B. Un incident grave
   C. Un quasi-incident à signaler
   D. Un incident de santé

2. 48 incidents dont 12 de gravité 3 ou 4. La part des incidents graves est :
   A. 12 %
   B. 25 %
   C. 36 %
   D. 4 %

3. 30 recommandations, 21 mises en œuvre dans les délais. Taux :
   A. 70 %
   B. 30 %
   C. 21 %
   D. 63 %

4. Dans une culture juste, un employé qui signale une erreur honnête :
   A. Est sanctionné pour l'exemple
   B. Est muté
   C. Doit rembourser les dégâts
   D. N'est pas sanctionné, et l'erreur sert à apprendre

5. Après l'enlèvement d'un employé, qui décide de la communication publique ?
   A. Le service communication du siège seul
   B. Chaque collègue sur les réseaux sociaux
   C. La cellule de crise
   D. Les médias locaux

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

Semaine 7 : Gérer une crise : cellule de crise, hibernation, relocalisation, évacuation, enlèvement

Objectifs

- Organiser une cellule de crise et ses premières heures : rôles, informations, décisions, journal.
- Planifier et décider une hibernation, une relocalisation ou une évacuation, y compris pour le personnel national.
- Connaître les principes de gestion d'un enlèvement ou d'une détention et le rôle de chacun.

Qu'est-ce qu'une crise ?

Une **crise** est une situation qui menace gravement les personnes, la capacité de l'organisation à fonctionner ou sa réputation, et qui dépasse les procédures ordinaires : enlèvement, décès violent, attaque d'une base, évacuation d'un pays, catastrophe touchant le personnel, scandale grave.

La gestion de crise s'appuie sur une structure préparée à l'avance :

- **Cellule de gestion de crise** (au siège ou au niveau régional) : décide de la stratégie, mobilise les ressources, gère les relations avec les familles, les autorités, les bailleurs et les médias.
- **Équipe de gestion de l'incident** (au niveau du pays) : gère la situation sur le terrain et applique les décisions.

Cette séparation permet au terrain de se concentrer sur l'action tandis que la cellule gère l'environnement et les décisions stratégiques. Les deux doivent avoir des mandats écrits, des membres désignés et des suppléants, et avoir fait au moins un exercice de simulation.

Les premières heures

Les premières heures déterminent souvent l'issue d'une crise. Liste d'actions type :

- **Activer** la cellule selon les critères prévus ; désigner un responsable et un secrétaire qui tient le **journal de crise** (heure, information, source, décision, responsable).
- **Établir les faits** : distinguer ce qui est confirmé, probable, rumeur.
- **Protéger les personnes** : mise en sécurité du reste du personnel, assistance médicale, regroupement.
- **Informer** les familles (par une personne désignée), le personnel, la direction ; contrôler la communication externe (aucun commentaire public sans décision de la cellule).
- **Prendre les décisions** urgentes : niveau de sécurité, suspension d'activités, mouvements.

- **Planifier** les prochaines heures et les relèves : une crise peut durer des semaines, la fatigue est un risque.

> Le journal de crise n'est pas une formalité : il garde la mémoire des décisions, protège l'organisation juridiquement et évite de refaire les mêmes discussions à chaque relève.

Hibernation, relocalisation, évacuation

Trois options quand la situation se dégrade, décrites dans le plan de sécurité :

- **Hibernation** : rester sur place, regroupés dans un lieu sûr, en attendant que le danger immédiat passe (combats dans la ville, émeutes). Exige des réserves (eau, nourriture, carburant, médicaments), des communications et une décision sur la durée maximale.
- **Relocalisation** : déplacer une partie du personnel vers une zone plus sûre du même pays (capitale, autre région), en général le personnel le plus exposé ou non essentiel.
- **Évacuation** : faire sortir le personnel du pays. Pour le personnel international, c'est souvent le retour dans le pays d'origine ; pour le personnel national, une évacuation hors du pays est juridiquement et pratiquement complexe, et rarement possible.

Le **point de non-retour** : passé un certain moment (aéroport fermé, routes coupées), l'évacuation n'est plus possible. Il faut donc décider **tôt**, sur la base des indicateurs, plutôt que d'attendre la certitude.

Calcul d'évacuation. 46 personnes à relocaliser par avion de 12 places ; 2 places réservées au personnel de la compagnie et au matériel de communication : 10 places utiles par rotation. Il faut 5 rotations. Si chaque rotation prend 3 heures et que l'aérodrome ferme à la tombée de la nuit, on ne peut faire que 3 rotations par jour : 2 jours au minimum. La liste de priorité (personnes les plus exposées, malades, non essentielles) est établie à l'avance.

Le personnel national dans les crises

Le personnel national est souvent le plus exposé et le moins protégé lors des crises. Les bonnes pratiques :

- Discuter à l'avance avec chaque employé de ses risques propres (profil, lieu d'origine, famille) et des options réalistes.
- Prévoir des options de **relocalisation interne** pour ceux qui sont menacés du fait de leur emploi.
- Garantir la **continuité des salaires** en cas de suspension (avances de salaire avant une évacuation, moyens de paiement à distance).
- Maintenir le **contact** et le soutien après le départ des internationaux.
- Ne pas transférer la responsabilité des programmes au personnel national ou aux partenaires sans ressources ni accord, en exposant ainsi ceux qui restent.

Exemple. Avant une évacuation, une organisation verse trois mois d'avance de salaire à ses 60 employés nationaux, organise un arbre d'appel quotidien, et convient avec eux d'un

protocole simple : aucune activité n'est maintenue sans évaluation et accord de chacun, et aucun employé ne garde de biens de l'organisation qui le mettraient en danger.

Enlèvement et détention

L'enlèvement est l'une des crises les plus graves et les plus longues. Principes généralement admis (à adapter à la politique de chaque organisation et au droit applicable) :

- **Prévention** : analyse des profils exposés, discrétion, variation des itinéraires et des horaires, contrôle des informations publiées (réseaux sociaux du personnel compris).
- **Préparation** : politique écrite (y compris la position de l'organisation sur les rançons, qui varie selon les organisations et les lois), formulaires « preuve de vie » confidentiels remplis à l'avance par le personnel exposé (questions dont seule la personne connaît la réponse), assurance spécialisée le cas échéant, consultants spécialisés identifiés.
- **Gestion** : cellule de crise dédiée, communication strictement contrôlée, coordination avec la famille et, selon les cas, avec les autorités et les gouvernements concernés, appui de spécialistes.
- **Après** : soutien médical et psychologique de longue durée pour la personne libérée et sa famille, ainsi que pour les collègues.

La **détention arbitraire** par des autorités ou des groupes armés exige une réaction rapide : localiser la personne, contacts avec les autorités, appui juridique, visites si possible, information de la famille.

Exercer et tirer les leçons

Une cellule de crise qui ne s'est jamais exercée perd des heures précieuses. Les **exercices** vont de la discussion autour d'un scénario (exercice sur table de 2 à 3 heures) à la simulation complète avec injections d'informations en temps réel.

Un bon exercice teste : l'activation (qui appelle qui, en combien de temps), la répartition des rôles, la circulation de l'information, la tenue du journal, les décisions difficiles (par exemple : informer ou non les médias, évacuer ou hiberner), et la relève.

Indicateur simple. Délai d'activation de la cellule : objectif inférieur à 2 heures. Lors d'un exercice, l'alerte est donnée à 22 h ; le premier membre est joint à 22 h 20, la cellule complète se réunit à 0 h 45 : 2 h 45, au-delà de l'objectif. Cause : la liste de contacts n'était pas à jour et deux suppléants n'étaient pas désignés. Action : mise à jour trimestrielle de la liste, suppléants nommés, test d'appel mensuel.

Après toute crise réelle, une **revue** (après au moins quelques semaines) examine ce qui a fonctionné et ce qui doit changer, avec la même culture d'apprentissage que pour les incidents.

Exercice d'application : la ville est encerclée

Situation. Des combats approchent d'une ville où l'organisation a 8 employés internationaux et 54 employés nationaux, dont 12 originaires d'une autre région et menacés en raison de leur groupe ethnique. L'aéroport fonctionne encore ; un avion de 14 places (12 places utiles) peut faire 2 rotations par jour vers la capitale. Les indicateurs du scénario « encerclement » sont 4 sur 6 réunis. La route vers la capitale est coupée. Les réserves de la résidence principale permettent 5 jours d'hibernation pour 20 personnes.

Travail demandé. 1) Hiberner, relocaliser ou évacuer, et pour qui ? 2) Combien de jours faut-il pour relocaliser les personnes prioritaires par avion ? 3) Quelles mesures pour le personnel national qui reste ?

Corrigé. 1) Avec 4 indicateurs sur 6 et une route coupée, le point de non-retour approche : relocaliser maintenant vers la capitale les personnes les plus exposées (les 12 employés menacés, avec leur accord) et le personnel international non essentiel ; garder une petite équipe essentielle seulement si l'hibernation est possible et sûre. 2) Personnes prioritaires : 12 employés menacés + 8 internationaux = 20 personnes, soit 2 rotations de 12 places, possibles en 1 jour. Si l'on ajoute des familles à charge des employés menacés (par exemple 16 personnes), 36 personnes = 3 rotations, soit 2 jours. 3) Avance de salaire de plusieurs mois, contact quotidien par arbre d'appel, aucune activité maintenue sans évaluation et accord, retrait des biens de l'organisation qui pourraient les exposer, information claire sur les options et soutien psychologique ; plan de reprise dès que la situation le permet.

À retenir

- Cellule de crise (stratégie, environnement) et équipe de terrain (action) : mandats, suppléants, exercices.
- Premières heures : activer, établir les faits, protéger, informer, décider, planifier ; tenir un journal.
- Hiberner, relocaliser, évacuer : décider avant le point de non-retour, sur indicateurs.
- Le personnel national, souvent le plus exposé, a droit à des options et à un soutien réels.
- Enlèvement : prévention, politique écrite, preuves de vie préparées, communication contrôlée, spécialistes.

Quiz

1. 30 personnes à relocaliser, avion de 10 places utiles. Nombre de rotations :
   A. 2
   B. 30
   C. 4
   D. 3

2. Hibernation de 15 personnes pendant 8 jours à 4 litres d'eau par personne et par jour :
   A. 120 litres
   B. 32 litres
   C. 480 litres
   D. 600 litres

3. Le journal de crise sert surtout à :
   A. Informer les médias
   B. Garder la trace des informations et des décisions, et faciliter les relèves
   C. Évaluer le personnel
   D. Calculer les coûts

4. Pourquoi préparer des formulaires « preuve de vie » à l'avance ?
   A. Pour vérifier, en cas d'enlèvement, que la personne est vivante grâce à des questions dont elle seule connaît la réponse
   B. Pour l'assurance santé
   C. Pour les visas
   D. Pour les ressources humaines

5. Une cellule de crise se réunit 3 h 10 après l'alerte, pour un objectif de 2 heures. Action prioritaire :
   A. Supprimer l'objectif
   B. Ne rien faire, c'était un exercice
   C. Changer de directeur
   D. Mettre à jour les contacts, désigner des suppléants et tester régulièrement

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

Semaine 8 : Santé, bien-être psychosocial, sauvegarde interne et assurances

Objectifs

- Organiser la protection de la santé du personnel : prévention, soins, évacuation médicale et premiers secours.
- Prévenir et prendre en charge le stress, l'épuisement et le traumatisme, et mesurer le bien-être des équipes.
- Traiter le harcèlement, les violences sexuelles contre le personnel et les besoins d'assurance comme des risques à part entière.

La santé, premier risque

Dans beaucoup de contextes, les **maladies** (paludisme, infections digestives, maladies chroniques mal suivies) et les **accidents** causent plus d'arrêts de travail, de rapatriements et parfois de décès que la violence. La protection de la santé fait donc partie de la gestion des risques.

Mesures essentielles :

- **Avant le départ ou l'affectation** : visite médicale, vaccinations, prophylaxie antipaludique adaptée, briefing santé du contexte.
- **Sur place** : cartographie des structures de soins (qualité, distance, horaires, langues), contrats avec des cliniques, trousses de premiers secours, personnel formé aux premiers secours (au moins une personne par équipe ou par véhicule en zone isolée).
- **Évacuation médicale** : procédure écrite, contrat avec un prestataire ou une assurance, critères de déclenchement, délais réalistes.
- **Personnel national** : couverture santé équivalente dans les faits, y compris pour les familles selon la politique de l'organisation.

Délai critique. La « première heure » après un traumatisme grave est décisive. Si l'hôpital chirurgical le plus proche est à 6 heures de route et qu'aucune évacuation aérienne n'est possible avant le lendemain, le risque d'accident grave pèse beaucoup plus lourd dans l'évaluation, et la formation aux premiers secours avancés devient prioritaire.

Stress, épuisement et traumatisme

Les travailleurs humanitaires sont exposés à trois types de stress :

- **Stress de base et cumulatif** : charge de travail, conditions de vie, isolement, conflits d'équipe, insécurité permanente. Non traité, il conduit à l'**épuisement** (burn-out).
- **Stress traumatique** : exposition à un événement violent ou à la mort.
- **Traumatisme vicariant** : à force d'écouter et de voir la souffrance des autres.

Plusieurs enquêtes auprès de travailleurs humanitaires ont mis en évidence des taux élevés de symptômes d'anxiété, de dépression et d'épuisement, souvent supérieurs à ceux de la population générale, et plus élevés encore chez le personnel national exposé aux mêmes violences que sa propre famille.

Mesures : charge de travail raisonnable, congés et pauses de récupération respectés (repos et récupération, R&R, selon le contexte, par exemple tous les 6 à 12 semaines en contexte difficile), accès confidentiel à un soutien psychologique, formation des responsables à repérer les signes, premiers secours psychologiques après un incident, culture qui ne stigmatise pas la demande d'aide.

> Un responsable qui ne prend jamais de congé envoie un message à toute son équipe. Le bien-être est aussi une affaire d'exemple.

Mesurer le bien-être

Le bien-être des équipes se mesure, comme tout risque :

- **Taux d'utilisation des congés** et des R&R : jours pris / jours dus.
- **Heures supplémentaires** moyennes et nombre de personnes au-delà d'un seuil.
- **Arrêts maladie** et rotation du personnel (départs anticipés).
- **Enquêtes anonymes** courtes et régulières (échelles validées de stress ou d'épuisement, questions sur le soutien perçu).
- Recours au **soutien psychologique** (en nombre, jamais en noms).

Exemple. Équipe de 40 personnes : 1 200 jours de congé dus sur l'année, 690 pris, soit 57,5 %. 14 personnes travaillent régulièrement plus de 55 heures par semaine. Rotation : 11 départs dans l'année, soit 27,5 %. Ces chiffres signalent un risque d'épuisement élevé : plan d'action (planification obligatoire des congés, renforts, réduction des réunions, suivi par la direction).

Harcèlement et violences sexuelles contre le personnel

Le **harcèlement** (moral et sexuel), la discrimination et les **violences sexuelles** contre le personnel, y compris par des collègues, sont des risques sous-déclarés. Ils relèvent à la fois de la sécurité, des ressources humaines et de la sauvegarde (safeguarding) interne.

Un dispositif minimal comprend :

- un **code de conduite** clair et signé, qui interdit aussi l'exploitation et les abus sexuels envers les populations ;
- des **canaux de signalement** multiples et confidentiels (y compris hors hiérarchie et externes) ;
- une approche **centrée sur la survivante ou le survivant** : sécurité, confidentialité, respect de ses choix, soins médicaux rapides (prophylaxie post-exposition au VIH et contraception d'urgence dans les délais), soutien psychologique ;

- des **enquêtes** menées par des personnes formées, indépendantes de la chaîne hiérarchique concernée ;
- des **sanctions** effectives et le partage d'informations entre organisations pour éviter le recrutement de personnes sanctionnées (dispositifs de vérification des références interorganisations).

Les kits de prophylaxie post-exposition doivent être disponibles et le personnel désigné formé à leur usage, car les délais d'efficacité sont courts (idéalement dans les premières heures, et au plus tard 72 heures).

Les assurances

Les assurances transfèrent une partie du risque financier. Couvertures habituelles :

- **Santé** (y compris à l'étranger) et **évacuation médicale** ;
- **Accident, invalidité et décès**, y compris pour les risques de guerre et de terrorisme, souvent exclus des contrats standard ;
- **Responsabilité civile** de l'organisation ;
- **Biens** : véhicules, équipements, stocks, argent liquide ;
- **Enlèvement et rançon** (kidnap and ransom), qui finance surtout les consultants spécialisés et dont l'existence doit rester confidentielle.

Points de vigilance : exclusions (zones, activités, guerre), plafonds, délais de déclaration, couverture équitable du personnel national, et cohérence avec le droit local (assurances obligatoires).

Calcul simple. Prime de 4 % de la masse salariale pour une couverture accident et décès incluant les risques de guerre, sur une masse salariale de 2 400 000 USD : 96 000 USD par an. Si l'organisation n'assure que les 30 internationaux (masse salariale 1 500 000 USD) et laisse 120 nationaux (900 000 USD) sans couverture équivalente, l'économie de 36 000 USD crée une inégalité grave et un risque juridique et réputationnel.

Les premiers secours et la préparation médicale

La préparation médicale de terrain se planifie comme le reste :

- **Formation** : premiers secours de base pour tous, premiers secours avancés en zone isolée ou de conflit (gestion des hémorragies, garrot, position latérale, brûlures).
- **Équipement** : trousse individuelle (pour les zones de conflit, avec garrot), trousse de véhicule, trousse de base.
- **Fiches médicales confidentielles** du personnel (groupe sanguin, allergies, traitements, contacts d'urgence), accessibles en cas d'urgence seulement.
- **Plan d'évacuation médicale** par zone : structure de première ligne, structure de référence, moyens de transport, délais, numéros, coût.

Calcul de besoins de formation. 85 employés en zone isolée, objectif : au moins 2 personnes formées aux premiers secours avancés par équipe de 5 en déplacement. Si 17

équipes peuvent être sur le terrain en même temps, il faut au moins 34 personnes formées ; avec 30 % de marge pour les absences et la rotation, environ 45 personnes.

Exercice d'application : une équipe à bout

Situation. Une base de 25 personnes (5 internationaux, 20 nationaux) en zone de conflit. Sur 6 mois : 3 départs anticipés d'internationaux, 4 arrêts maladie longs chez les nationaux ; 210 jours de congé pris sur 450 dus ; le chef de base n'a pris aucun congé ; une employée nationale a signalé à une collègue des avances répétées d'un superviseur, mais ne veut pas « faire d'histoires ». L'hôpital chirurgical le plus proche est à 5 heures de route ; aucune personne n'est formée aux premiers secours avancés. L'assurance décès et invalidité couvre uniquement les internationaux.

Travail demandé. 1) Calculez le taux d'utilisation des congés. 2) Identifiez les risques. 3) Proposez des mesures prioritaires.

Corrigé. 1) 210 / 450 = 46,7 %. 2) Épuisement collectif (congés peu pris, départs et arrêts, exemple du chef de base) ; harcèlement sexuel signalé de façon informelle, avec risque d'escalade et de silence ; risque médical grave (5 heures de l'hôpital, aucun secouriste avancé) ; inégalité de couverture d'assurance. 3) Planification obligatoire des congés et R&R, en commençant par le chef de base ; soutien psychologique accessible et confidentiel ; informer l'employée, sans la forcer, des canaux de signalement confidentiels et de ses options, garantir sa sécurité et l'absence de représailles, et faire intervenir la fonction sauvegarde selon la politique (une alerte reçue par un responsable ne peut pas être ignorée) ; former rapidement au moins 2 personnes par équipe aux premiers secours avancés et réviser le plan d'évacuation médicale ; étendre l'assurance au personnel national.

À retenir

- Maladies et accidents pèsent souvent plus que la violence : prévention, soins, évacuation médicale planifiés.
- Stress cumulatif, traumatique et vicariant : congés, R&R, soutien confidentiel, exemple des responsables.
- Mesurer le bien-être : congés pris, heures, arrêts, rotation, enquêtes anonymes.
- Harcèlement et violences sexuelles : canaux confidentiels, approche centrée sur la survivante ou le survivant, PEP sous 72 heures.
- Assurances adaptées aux risques de guerre, et équitables entre personnels nationaux et internationaux.

Quiz

1. Une équipe a pris 540 jours de congé sur 900 dus. Taux d'utilisation :
   A. 60 %
   B. 40 %
   C. 54 %
   D. 90 %

2. La prophylaxie post-exposition au VIH doit être commencée au plus tard dans les :
   A. 7 jours
   B. 2 semaines
   C. 30 jours
   D. 72 heures

3. Masse salariale 1 800 000 USD, prime de 3 %. Coût annuel :
   A. 5 400 USD
   B. 18 000 USD
   C. 54 000 USD
   D. 540 000 USD

4. Le traumatisme vicariant est causé par :
   A. Un accident de la route
   B. L'exposition répétée à la souffrance des autres
   C. Un surcroît de congés
   D. Le décalage horaire

5. Un responsable reçoit une alerte informelle de harcèlement sexuel. Il :
   A. Informe la victime de ses options et des canaux confidentiels et active la procédure de sauvegarde
   B. Attend une plainte écrite
   C. Confronte publiquement l'auteur présumé
   D. Ignore si la victime ne veut pas faire d'histoires

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

Semaine 9 : Sécurité numérique et protection de l'information

Objectifs

- Identifier les menaces numériques propres aux organisations humanitaires : hameçonnage, fraude au virement, surveillance, fuite de données.
- Mettre en place des mesures de base proportionnées : authentification, sauvegardes, chiffrement, gestion des accès, appareils.
- Protéger les données des personnes aidées et du personnel, et réagir à un incident numérique.

Pourquoi le numérique est un risque de sécurité

Les organisations humanitaires détiennent des informations très sensibles : listes de bénéficiaires (parfois avec biométrie et localisation), témoignages de violations, données médicales, informations sur le personnel, analyses de sécurité, mouvements. Une fuite ou un piratage peut mettre des **vies** en danger, pas seulement des données.

Plusieurs cyberattaques connues ont visé des organisations humanitaires, y compris le vol de données de centaines de milliers de personnes vulnérables. Les organisations sont aussi visées par la fraude financière en ligne et par la **surveillance** des communications par des acteurs étatiques ou non étatiques.

Menaces principales :

- **Hameçonnage** (phishing) : faux courriels ou messages qui volent des identifiants ou installent des logiciels malveillants.
- **Fraude au virement** : faux fournisseur, faux directeur demandant un paiement urgent, changement frauduleux de coordonnées bancaires.
- **Rançongiciel** : chiffrement des données contre rançon.
- **Vol ou saisie d'appareils** (ordinateurs, téléphones) aux points de contrôle ou lors de braquages.
- **Surveillance** des communications et des réseaux sociaux.
- **Erreurs internes** : partage par erreur, fichier envoyé au mauvais destinataire, mot de passe affiché.

Les mesures de base

Quelques mesures simples bloquent la grande majorité des attaques courantes :

- **Authentification à plusieurs facteurs** (MFA) sur la messagerie, le stockage en ligne, la banque et le logiciel comptable.
- **Gestionnaire de mots de passe** et mots de passe longs et uniques.
- **Mises à jour** automatiques des systèmes et des applications.

- **Sauvegardes** régulières, dont une copie hors ligne ou isolée, et tests de restauration (règle 3-2-1 : trois copies, deux supports différents, une copie hors site).
- **Chiffrement** des disques des ordinateurs portables et des téléphones.
- **Gestion des accès** : chacun n'accède qu'à ce dont il a besoin ; retrait des accès le jour du départ d'un employé.
- **Formation** régulière, avec des exercices d'hameçonnage simulés.

Exemple d'exercice. Un faux courriel d'hameçonnage est envoyé à 120 employés : 38 cliquent sur le lien (31,7 %), 14 saisissent leurs identifiants (11,7 %), 9 signalent le courriel au service informatique (7,5 %). Après une formation ciblée, un second exercice donne 12 clics (10 %), 3 saisies (2,5 %) et 41 signalements (34,2 %). La hausse des signalements est aussi importante que la baisse des clics : elle transforme le personnel en système d'alerte.

Fraude au virement et procédures financières

La **fraude au président** et la fraude aux coordonnées bancaires coûtent chaque année des sommes importantes aux organisations, y compris humanitaires. Les procédures financières sont la meilleure défense :

- Toute **modification de coordonnées bancaires** d'un fournisseur ou d'un employé est vérifiée par un appel à un numéro déjà connu, jamais à celui indiqué dans la demande.
- Aucun paiement urgent hors procédure, même à la demande apparente d'un directeur : la double validation reste obligatoire.
- Les accès à la banque en ligne utilisent des appareils et des comptes dédiés, avec double signature électronique.
- Le personnel sait qu'il sera **soutenu** s'il refuse un paiement suspect, même demandé par un supérieur.

> L'urgence et la confidentialité sont les deux leviers favoris des fraudeurs : « Je suis en réunion, fais ce virement tout de suite et n'en parle à personne. »

Appareils, points de contrôle et surveillance

Sur le terrain, les risques numériques sont aussi **physiques** :

- Aux points de contrôle, les téléphones peuvent être fouillés. Un téléphone qui contient des photos de positions militaires, des messages critiques envers une partie ou des listes de bénéficiaires peut entraîner une détention. Règle : ne transporter que le nécessaire, supprimer les données sensibles des appareils de terrain, utiliser des appareils dédiés au travail.
- Les **réseaux sociaux** du personnel révèlent des informations exploitables : localisation en temps réel, opinions politiques, photos de collègues, signes de richesse. Une politique sur l'usage des réseaux sociaux, expliquée et non punitive, réduit ces risques.
- Les **messageries** chiffrées de bout en bout protègent le contenu, mais pas le fait que l'on communique, ni le téléphone lui-même s'il est saisi déverrouillé.

- L'usage de certains outils (satellites, VPN, drones) peut être interdit ou suspect : vérifier la législation et l'acceptation.

Protéger les données des personnes

La **protection des données** des bénéficiaires et du personnel repose sur des principes reconnus (notamment le manuel du CICR et du Brussels Privacy Hub sur la protection des données dans l'action humanitaire) :

- **Licéité et finalité** : base légitime et finalité précise pour chaque collecte.
- **Minimisation** : ne collecter que ce qui est nécessaire.
- **Consentement éclairé** lorsque c'est la base retenue, en tenant compte des rapports de pouvoir (un ménage qui a besoin d'aide n'est pas libre de refuser).
- **Sécurité** : chiffrement, accès limités, journalisation.
- **Conservation limitée** et suppression à la fin de la finalité.
- **Partage encadré** par des accords de partage de données, avec une analyse des risques (y compris des demandes d'autorités ou de parties au conflit).
- **Analyse d'impact** avant tout nouveau système (biométrie, paiement mobile, plateforme partagée).

Exemple de minimisation. Pour une distribution de kits, il faut identifier le ménage et vérifier qu'il n'a pas déjà reçu le kit. L'appartenance ethnique ou religieuse n'est pas nécessaire et ne doit pas être collectée ; la photo et l'empreinte digitale ne le sont généralement pas non plus.

Réagir à un incident numérique

Un incident numérique (compte piraté, ordinateur volé, rançongiciel, fichier envoyé par erreur) se traite comme un incident de sécurité :

- **Contenir** : changer les mots de passe, révoquer les sessions, isoler l'appareil infecté, effacer à distance un appareil volé.
- **Évaluer** : quelles données, quelles personnes, quel risque pour elles ?
- **Informer** : direction, responsable de la protection des données, personnes concernées si elles sont exposées à un risque, autorités de contrôle selon le droit applicable, bailleurs selon les contrats.
- **Restaurer** à partir des sauvegardes ; ne pas payer une rançon sans décision de la direction et analyse juridique.
- **Apprendre** : analyse, corrections, formation.

Exemple. Un ordinateur portable non chiffré contenant la liste de 3 200 ménages avec leurs numéros de téléphone et leur localisation est volé lors d'un braquage. Le risque pour les personnes dépend du contexte : si certains ménages appartiennent à un groupe ciblé, il est élevé. Actions : évaluation immédiate, information des communautés concernées par des canaux sûrs si elles sont exposées, changement des modalités de contact, chiffrement obligatoire de tous les ordinateurs portables.

Exercice d'application : un courriel urgent du directeur

Situation. Un vendredi à 17 h, la comptable reçoit un courriel apparemment du directeur pays, en déplacement : « Confidentiel. Nous devons payer aujourd'hui l'acompte de 48 000 USD au nouveau fournisseur de carburant, sinon nous perdons le contrat. Coordonnées bancaires ci-jointes. Je ne suis pas joignable, réunion avec le ministre. » L'adresse d'envoi diffère d'une lettre de l'adresse habituelle. Le même jour, un fournisseur habituel a demandé par courriel de changer ses coordonnées bancaires. La messagerie de l'organisation n'a pas d'authentification à deux facteurs.

Travail demandé. 1) Signaux d'alerte. 2) Conduite immédiate. 3) Mesures durables.

Corrigé. 1) Urgence, confidentialité, indisponibilité du demandeur, nouveau fournisseur sans dossier d'achat, adresse d'envoi légèrement différente, demande parallèle de changement de coordonnées bancaires. 2) Ne pas payer ; appeler le directeur sur son numéro connu (ou son adjoint) ; ne pas modifier les coordonnées du fournisseur habituel sans appel de vérification à un numéro déjà connu ; signaler au responsable informatique et à la finance ; conserver les courriels comme preuves. 3) Authentification à deux facteurs sur toute la messagerie ; règle écrite : aucun paiement hors procédure, double validation, vérification téléphonique de toute modification bancaire ; formation et exercices d'hameçonnage ; filtrage des domaines ressemblants ; message clair de la direction : refuser un paiement suspect sera toujours soutenu.

À retenir

- Les données humanitaires sont sensibles : une fuite peut mettre des vies en danger.
- MFA, mots de passe uniques, mises à jour, sauvegardes 3-2-1, chiffrement, accès minimaux, formation.
- Fraude au virement : vérification par un numéro connu, double validation, soutien à qui refuse.
- Terrain : appareils allégés aux points de contrôle, politique sur les réseaux sociaux.
- Protection des données : finalité, minimisation, sécurité, conservation limitée, analyse d'impact.

Quiz

1. 150 employés reçoivent un faux courriel ; 24 cliquent. Taux de clic :
   A. 24 %
   B. 16 %
   C. 6,25 %
   D. 15 %

2. La règle de sauvegarde 3-2-1 signifie :
   A. 3 copies, 2 supports différents, 1 copie hors site
   B. 3 mots de passe, 2 facteurs, 1 compte
   C. 3 jours, 2 semaines, 1 mois
   D. 3 serveurs, 2 pays, 1 cloud

3. Un fournisseur demande par courriel de changer ses coordonnées bancaires. Vous :
   A. Changez immédiatement
   B. Payez en espèces
   C. Répondez au courriel
   D. Vérifiez par un appel au numéro déjà connu

4. Pour une distribution de kits, collecter l'appartenance ethnique des ménages est :
   A. Obligatoire
   B. Recommandé
   C. Contraire au principe de minimisation si ce n'est pas nécessaire
   D. Sans risque

5. Un ordinateur non chiffré contenant des listes de bénéficiaires est volé. Première étape :
   A. Racheter un ordinateur
   B. Évaluer les données exposées et le risque pour les personnes, puis informer
   C. Ne rien dire
   D. Publier un communiqué

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

Semaine 10 : Gérer tous les risques de l'organisation : registre, appétit, conformité et réputation

Objectifs

- Construire et tenir un registre des risques de l'organisation (sécurité, fiduciaire, opérationnel, juridique, réputationnel, éthique).
- Définir l'appétit pour le risque et le traduire en seuils et en décisions, y compris par la perte attendue.
- Intégrer la conformité (sanctions, antiterrorisme, fraude, protection contre l'exploitation et les abus sexuels) dans une approche unique.

Des risques de sécurité aux risques de l'organisation

La gestion des risques de l'organisation (souvent appelée ERM, enterprise risk management) élargit la logique de la sécurité à tous les risques qui menacent la mission :

- **Sécurité** : violence, accidents, santé du personnel.
- **Fiduciaires** : fraude, corruption, détournement, mauvaise utilisation des fonds.
- **Opérationnels** : rupture d'approvisionnement, défaillance d'un partenaire, perte d'accès.
- **Juridiques et de conformité** : sanctions, antiterrorisme, droit du travail, fiscalité, protection des données.
- **Éthiques et de sauvegarde** : exploitation et abus sexuels, harcèlement, atteinte aux principes.
- **Réputationnels** : perte de confiance des communautés, des bailleurs et du public.
- **Financiers et stratégiques** : dépendance à un bailleur, crise de trésorerie, perte de pertinence.

Ces risques sont **liés** : un détournement d'aide par un groupe armé est à la fois fiduciaire, juridique (sanctions), opérationnel (suspension), réputationnel et de sécurité (représailles si l'organisation le dénonce). C'est pourquoi une approche intégrée est nécessaire.

Le registre des risques

Le **registre des risques** recense les principaux risques, avec pour chacun : description (cause, événement, conséquence), catégorie, propriétaire, probabilité, impact, score inhérent, mesures existantes, score résiduel, mesures supplémentaires prévues, échéance.

Risque	Propriétaire	Inhérent	Résiduel	Action
Détournement d'aide alimentaire par une autorité locale dans la province X	Directeur des programmes	4 × 5 = 20	3 × 4 = 12	Vérification par des tiers, appels aux bénéficiaires, distribution directe
Fraude dans les achats de carburant	Directeur financier	4 × 3 = 12	2 × 3 = 6	Cartes carburant, rapprochements mensuels
Perte du premier bailleur (55 % des revenus)	Directeur général	3 × 5 = 15	3 × 4 = 12	Plan de diversification, réserves
Exploitation sexuelle par un employé ou un partenaire	Responsable sauvegarde	3 × 5 = 15	2 × 5 = 10	Formation, vérification des références, canaux de plainte communautaires

Le registre est revu chaque trimestre par la direction et chaque année par le conseil ou son comité d'audit et des risques. Les **dix principaux risques** font l'objet d'un suivi particulier.

L'appétit pour le risque

L'**appétit pour le risque** est le niveau de risque que l'organisation accepte de prendre pour atteindre sa mission. Il est fixé par le conseil, par catégorie :

- **Sécurité** : appétit modéré, élevé seulement pour les activités vitales (voir la criticité des programmes).
- **Fiduciaire** : appétit faible pour la fraude, mais acceptation d'un risque résiduel dans les contextes difficiles, à condition de le détecter et de le signaler.
- **Exploitation et abus sexuels** : tolérance zéro pour les comportements, ce qui n'empêche pas de reconnaître que le risque existe et doit être géré activement.
- **Programmatique** : appétit plus élevé pour l'innovation et l'accès à des zones difficiles.

L'appétit pour le risque n'est pas un slogan : il se traduit en **seuils** (score résiduel maximal par catégorie), en **délégations** (qui peut accepter quel niveau de risque) et en **décisions** documentées. Un appétit trop faible empêche de travailler là où les besoins sont les plus grands ; un appétit non défini laisse chaque responsable décider seul.

La perte attendue

Pour certains risques financiers, on peut compléter la matrice par la **perte attendue** : probabilité annuelle × coût en cas de réalisation. Cela aide à comparer le coût d'une mesure à la perte qu'elle évite.

Exemple. Risque de vol de la caisse d'un bureau de terrain : probabilité annuelle estimée à 20 %, perte moyenne 15 000 USD (espèces et frais). Perte attendue : 0,2 × 15 000 = 3 000 USD par an. Passer aux paiements par mobile money coûte 1 800 USD par an et réduit la probabilité à 5 % et la perte moyenne à 4 000 USD : perte attendue 200 USD. Gain net : 3 000 − 200 − 1 800 = 1 000 USD par an, sans compter la baisse du risque pour la sécurité du caissier.

Limites : la perte attendue ne convient pas aux risques qui touchent des vies ou dont l'impact est catastrophique. Personne ne décide d'accepter un enlèvement parce que sa « perte attendue » serait faible. Pour ces risques, on raisonne en seuil acceptable et en plans de contingence.

Conformité : sanctions, antiterrorisme, fraude

Les obligations de conformité s'imposent par les lois nationales, les régimes de sanctions et les contrats des bailleurs :

- **Sanctions et antiterrorisme** : interdiction de mettre des fonds ou des ressources à la disposition de personnes ou entités inscrites sur les listes. Mesures : vérification des fournisseurs, partenaires, employés selon le risque ; clauses contractuelles ; vigilance sur les paiements dans les zones contrôlées par des groupes listés ; usage des exemptions humanitaires existantes en documentant leur application.
- **Antifraude et anticorruption** : politique, ligne d'alerte, enquêtes, signalement aux bailleurs dans les délais (voir la finance).
- **Vérification du bénéficiaire final** : en général, les bailleurs n'exigent pas de vérifier chaque bénéficiaire de l'aide contre les listes, et les principes humanitaires s'y opposent ; les contrôles portent sur les partenaires, fournisseurs et personnels.

Le dialogue avec les bailleurs et les banques est essentiel : le **retrait des banques** (de-risking), qui refusent de traiter avec des organisations travaillant dans des zones sanctionnées, peut bloquer des opérations entières. Documenter sa diligence aide à garder les comptes ouverts.

Protection contre l'exploitation et les abus sexuels

La **protection contre l'exploitation et les abus sexuels** (PSEA) envers les populations aidées est une obligation fondamentale. Les six principes fondamentaux du Comité permanent interorganisations (IASC) interdisent notamment toute relation sexuelle avec des enfants (moins de 18 ans), tout échange d'argent, d'emploi, de biens ou de services contre des faveurs sexuelles, et imposent de signaler toute préoccupation.

Le dispositif :

- code de conduite et formation de tout le personnel et des partenaires ;
- vérification des références au recrutement (dispositifs interorganisations) ;
- **mécanismes de plainte communautaires** accessibles, sûrs, adaptés aux femmes et aux enfants ;
- assistance aux victimes (médicale, psychosociale, juridique) selon leurs choix ;
- enquêtes rapides et indépendantes, sanctions, signalement aux bailleurs ;
- clauses PSEA dans les accords avec les partenaires.

Indicateur trompeur : **zéro plainte** ne signifie pas zéro abus. Dans la plupart des contextes, l'absence de plaintes indique plutôt que les mécanismes ne sont ni connus ni jugés sûrs par les communautés.

Exercice d'application : le comité des risques du conseil

Situation. Vous présentez au comité des risques d'une ONG les éléments suivants. Fraude au carburant : probabilité annuelle 30 %, perte moyenne 25 000 USD ; mesure proposée (cartes carburant et rapprochements) coûtant 4 000 USD par an, qui réduirait la probabilité à 10 % et la perte à 10 000 USD. Détournement d'aide dans une province : inhérent 4 × 5, résiduel 3 × 4 ; seuil d'appétit fiduciaire du conseil : résiduel ≤ 9. Mécanisme de plainte PSEA : aucune plainte en 2 ans sur 5 provinces ; une enquête de connaissance montre que 18 % des femmes interrogées connaissent le mécanisme. Un partenaire local n'a jamais été vérifié contre les listes de sanctions.

Travail demandé. 1) La mesure carburant est-elle justifiée ? 2) Le risque de détournement est-il dans l'appétit ? Que faire ? 3) Que conclure sur la PSEA ? 4) Le partenaire ?

Corrigé. 1) Perte attendue actuelle : 0,3 × 25 000 = 7 500 USD ; après mesure : 0,1 × 10 000 = 1 000 USD ; gain net : 7 500 − 1 000 − 4 000 = 2 500 USD par an : justifiée. 2) Résiduel 12 > 9 : hors appétit. Options : mesures supplémentaires (vérification par des tiers, distribution directe, transferts monétaires), réduction du volume dans la province, ou acceptation explicite et documentée par le conseil d'un dépassement temporaire avec plan. 3) Zéro plainte avec 18 % de connaissance indique un mécanisme inefficace, pas une absence d'abus : campagne d'information, canaux adaptés aux femmes, points focaux féminins, vérification de la confiance des communautés. 4) Vérification immédiate contre les listes de sanctions, et intégration systématique de cette vérification dans la procédure de sélection des partenaires.

À retenir

- Les risques de l'organisation sont liés : sécurité, fiduciaire, opérationnel, juridique, éthique, réputationnel, financier.
- Registre des risques avec propriétaires, scores inhérents et résiduels, actions et échéances, revu par la direction et le conseil.
- Appétit pour le risque fixé par le conseil, par catégorie, traduit en seuils et en délégations.
- Perte attendue = probabilité × coût : utile pour les risques financiers, pas pour les vies.
- PSEA : zéro plainte n'est pas zéro abus ; sanctions : vérifier partenaires, fournisseurs et personnel.

Quiz

1. Probabilité annuelle 25 %, perte 12 000 USD. Perte attendue :
   A. 12 000 USD
   B. 4 800 USD
   C. 3 000 USD
   D. 300 USD

2. Une mesure coûte 2 000 USD par an et réduit la perte attendue de 5 000 à 1 500 USD. Gain net annuel :
   A. 3 500 USD
   B. 1 500 USD
   C. 5 000 USD
   D. −500 USD

3. Qui fixe l'appétit pour le risque de l'organisation ?
   A. Le conseil d'administration
   B. Chaque chef de projet
   C. Le bailleur principal
   D. L'auditeur externe

4. Un mécanisme de plainte PSEA ne reçoit aucune plainte en deux ans. Conclusion la plus probable :
   A. Il n'y a aucun abus
   B. Il faut supprimer le mécanisme
   C. Le personnel est exemplaire
   D. Le mécanisme n'est probablement ni connu ni jugé sûr

5. Les vérifications contre les listes de sanctions portent en général sur :
   A. Chaque bénéficiaire de l'aide
   B. Les journalistes
   C. Les partenaires, fournisseurs et personnels selon le risque
   D. Personne

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

Semaine 11 : Partager le risque avec les partenaires et financer la sécurité

Objectifs

- Analyser le transfert de risque vers les partenaires nationaux et locaux et construire un partage équitable des risques.
- Budgéter la sécurité de façon complète et la défendre auprès des bailleurs.
- Organiser la sécurité dans les consortiums, la gestion à distance et la coordination interorganisations.

Le transfert du risque

Quand l'accès devient difficile, les organisations internationales s'appuient de plus en plus sur des **partenaires nationaux et locaux**, mieux acceptés et souvent seuls présents. C'est une force pour la réponse et pour la localisation, mais cela peut devenir un **transfert de risque** : l'organisation internationale réduit son exposition en exposant davantage le partenaire, sans lui donner les moyens d'y faire face.

Signes d'un transfert injuste :

- le partenaire travaille dans des zones où l'organisation internationale interdit à son propre personnel de se rendre, sans évaluation conjointe des risques ;
- le budget du partenaire ne contient aucune ligne de sécurité (communications, assurances, formation, véhicules adaptés) ;
- le partenaire supporte seul le risque fiduciaire (pertes et vols remboursés par lui) et le risque juridique (sanctions) ;
- aucune assistance n'est prévue en cas d'incident grave touchant le personnel du partenaire.

Vers un partage équitable

Le **partage du risque** (risk sharing) est une approche qui reconnaît que les risques doivent être répartis selon la capacité de chacun à les gérer, et financés. Les travaux interorganisations sur ce sujet (notamment dans le cadre du Grand Bargain et des réseaux d'ONG) proposent :

- une **évaluation conjointe** des risques avec le partenaire, avant l'accord ;
- des **coûts de sécurité éligibles** dans le budget du partenaire, à hauteur des besoins réels ;
- un accès du partenaire à la **formation**, aux analyses de sécurité et aux dispositifs d'urgence (évacuation médicale, assurance) ;
- un partage clair du **risque fiduciaire** : quelles pertes sont acceptées si les procédures ont été suivies, et lesquelles sont remboursées ;

- des **engagements réciproques** en cas d'incident grave : assistance, communication, soutien aux familles.

> Question test : si cet incident arrivait à notre propre personnel, que ferions-nous ? Le partenaire mérite-t-il moins ?

Budgéter la sécurité

La sécurité coûte, et ses coûts doivent apparaître clairement dans les budgets, sinon ils sont pris ailleurs ou ignorés. Postes typiques :

- **Personnel** : conseiller sécurité, points focaux, gardes, opérateurs radio.
- **Équipements** : communications (radios, téléphones satellitaires, balises), véhicules adaptés, protections des sites, équipements de protection individuelle selon le contexte.
- **Formation** : sécurité de base, formations avancées, premiers secours, exercices de crise.
- **Services** : abonnements à des services d'analyse, forums de sécurité, évacuation médicale, assurances spécifiques.
- **Réserves de contingence** : hibernation, relocalisation, évacuation.

Exemple de budget annuel d'un pays (8 millions USD de programmes, 150 employés). Conseiller sécurité et 3 points focaux : 140 000 ; gardes (6 sites) : 90 000 ; communications : 45 000 ; formation et exercices : 35 000 ; adaptations des sites : 40 000 ; assurances spécifiques et évacuation médicale : 60 000 ; contingence : 30 000. Total : 440 000 USD, soit 5,5 % des programmes et environ 2 933 USD par employé. Ce pourcentage varie fortement selon les contextes, souvent de 2 à 15 %.

Défendre le budget de sécurité

Les bailleurs acceptent généralement les coûts de sécurité s'ils sont **justifiés, proportionnés et liés à l'accès**. Arguments efficaces :

- relier chaque coût à un risque identifié dans l'évaluation des risques et à une activité ;
- montrer ce que la sécurité permet : accès à des zones précises, continuité des activités, protection des personnes aidées ;
- présenter les coûts en coûts directs du projet (au prorata, selon des clés justifiables) plutôt que de les noyer dans les coûts indirects ;
- montrer les données : incidents évités ou mieux gérés, jours d'activité maintenus.

Exemple d'argument chiffré. L'an dernier, sans téléphones satellitaires, les équipes de deux bases ont suspendu leurs déplacements 45 jours au total à chaque coupure du réseau mobile. Équiper ces bases coûte 12 000 USD ; les 45 jours de suspension ont retardé des activités d'une valeur de 300 000 USD. L'investissement est faible au regard de la continuité qu'il permet.

Consortiums, gestion à distance et coordination

Dans un consortium, chaque membre reste responsable de son personnel, mais le chef de file doit s'assurer que les risques sont évalués et gérés par tous : évaluation commune, partage d'informations, procédures d'alerte communes, budget de sécurité pour chaque membre.

En gestion à distance, la sécurité des équipes sur place (personnel national, partenaires) devient prioritaire : analyse locale par ceux qui sont exposés, droit de refuser une activité, communications, moyens de relocalisation, et contacts réguliers.

Coordination interorganisations :

- Les **forums de sécurité des ONG** (plateformes nationales de partage d'informations et d'analyses, souvent financées par des bailleurs) : alertes, rapports d'incidents, formations, analyses.
- Le cadre **« Saving Lives Together »** qui organise la coopération entre le système de gestion de la sécurité des Nations unies et les ONG partenaires.
- Le **Global Interagency Security Forum** (GISF) au niveau international : guides, recherches, échanges entre responsables sécurité.

Le partage d'informations exige des règles : confidentialité, anonymisation, accord préalable pour toute donnée qui n'appartient pas à l'organisation.

Mesurer la maturité de la gestion des risques

Une organisation peut évaluer sa **maturité** en gestion des risques de sécurité sur quelques dimensions, notées de 1 (inexistant) à 4 (intégré et amélioré en continu) :

- politique et gouvernance (seuil de risque, responsabilités) ;
- évaluation des risques et plans à jour ;
- formation et compétences ;
- incidents et apprentissage ;
- gestion de crise ;
- devoir de protection équitable (personnel national, partenaires) ;
- ressources et budget.

Exemple. Notes d'une organisation : 3, 2, 2, 1, 3, 1, 2. Moyenne : 14 / 7 = 2. Les deux notes de 1 (incidents et apprentissage ; devoir de protection équitable) sont les priorités : elles touchent la capacité à apprendre et l'équité, sur lesquelles reposent les autres dimensions. Une auto-évaluation annuelle, discutée au conseil, permet de suivre les progrès.

Exercice d'application : un partenaire en première ligne

Situation. Votre organisation finance une ONG locale pour des activités de protection de l'enfance dans une province où votre personnel n'est plus autorisé à se rendre. Le budget du partenaire (600 000 USD) ne prévoit aucun coût de sécurité. Le partenaire a 40 employés sur place ; deux d'entre eux ont été détenus 3 jours le mois dernier ; il n'a ni assurance accident ni téléphone satellitaire. L'accord prévoit que toute perte de biens, même due à un pillage, est remboursée par le partenaire.

Travail demandé. 1) Identifiez les problèmes. 2) Proposez un budget de sécurité réaliste pour le partenaire (communications 6 000 ; formation 8 000 ; assurance accident 3 % d'une masse salariale de 240 000 ; réserve de contingence 10 000 ; point focal sécurité à mi-temps 9 000). 3) Quelles modifications de l'accord ?

Corrigé. 1) Transfert de risque injuste : zone jugée trop dangereuse pour votre personnel, sans évaluation conjointe ; aucun coût de sécurité ; détention sans soutien prévu ; risque fiduciaire entièrement transféré, y compris pour une force majeure. 2) Communications 6 000 + formation 8 000 + assurance 7 200 + contingence 10 000 + point focal 9 000 = 40 200 USD, soit 6,7 % du budget ; à financer en plus ou par réallocation, en le justifiant auprès du bailleur. 3) Évaluation conjointe des risques et droit du partenaire de suspendre une activité dangereuse ; ligne budgétaire sécurité ; accès aux formations, aux analyses et à l'évacuation médicale de votre organisation ; clause de partage du risque fiduciaire (pertes dues au pillage acceptées si procédures suivies et incident signalé) ; engagement d'assistance en cas de détention ou d'incident grave.

À retenir

- Travailler avec des partenaires ne doit pas devenir un transfert injuste du risque.
- Partage du risque : évaluation conjointe, budget de sécurité, accès aux formations et dispositifs, pertes partagées.
- Budgéter la sécurité en coûts directs, liés aux risques et aux activités, souvent 2 à 15 % selon le contexte.
- Défendre la sécurité par l'accès et la continuité qu'elle permet, chiffres à l'appui.
- Forums de sécurité des ONG, Saving Lives Together, GISF : coordination avec des règles de confidentialité.

Quiz

1. Budget de sécurité 360 000 USD pour 6 000 000 USD de programmes. Part :
   A. 3,6 %
   B. 0,6 %
   C. 16,7 %
   D. 6 %

2. Même budget pour 120 employés. Coût par employé :
   A. 300 USD
   B. 50 000 USD
   C. 3 000 USD
   D. 30 000 USD

3. Un partenaire rembourse seul toute perte due à un pillage, même si les procédures ont été suivies. C'est :
   A. Un partage équitable
   B. Un transfert injuste du risque fiduciaire
   C. Une bonne pratique
   D. Une exigence de tous les bailleurs

4. Notes de maturité 2, 3, 1, 2, 2 sur 5 dimensions. Moyenne :
   A. 2
   B. 2,5
   C. 1,8
   D. 10

5. Dans un consortium, la sécurité du personnel de chaque membre relève :
   A. Du chef de file uniquement
   B. Des autorités locales
   C. Du bailleur
   D. De chaque membre, avec un dispositif coordonné par le chef de file

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

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