MANUEL DE GESTION DE L'INFORMATION ISSUE DES INCIDENTS DE SÉCURITÉ

TREIZE OUTILS POUR VOTRE ORGANISATION

Funded by European Union Humanitarian Aid

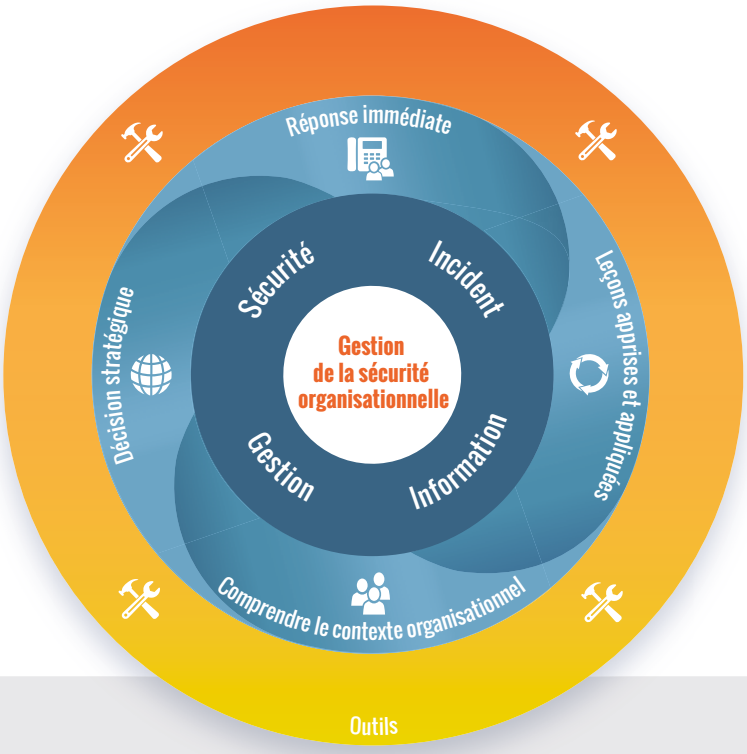
eisf

redr uk
people and skills for disaster relief

Aid in Danger

Insecurity Insight
Data on People in Danger

CHAPITRE 3 : OUTILS



Cette section contient des outils d'aide à la gestion de l'information issue des incidents de sécurité. Ils doivent être lus et utilisés conjointement avec le contenu écrit de ce manuel. Les outils sont organisés comme suit (cliquez sur l'élément pour accéder à l'outil) :

- Outil 1 : Grille d'auto-évaluation GIIS
- Outil 2 : Typologie des incidents
- Outil 3 : Incident organisationnel ou externe
- Outil 4 : Modèle de rapport d'incident
- Outil 5 : Grilles d'analyse des incidents
- Outil 6 : Comment effectuer un débriefing factuel
- Outil 7 : Bonnes pratiques en matière de signalement des incidents liés au genre et mécanismes de plainte pour signaler l'exploitation et les abus sexuels (EAS)
- Outil 8 : Plan d'action pour le suivi des incidents
- Outil 9 : Systèmes GIIS
- Outil 10 : Conservation de l'information issue des incidents
- Outil 11 : Technologie pour signaler et enregistrer les incidents
- Outil 12 : Analyse et comparaison des tendances des données
- Outil 13 : Questions de niveau stratégique pour les décisions relatives à la gestion de l'information issue des incidents de sécurité

OUTIL 1 : GRILLES D'AUTO-ÉVALUATION

Veuillez utiliser ce tableau comme guide pour les éléments typiques d'un système de gestion de l'information issue des incidents.

QUESTIONS GÉNÉRALES	
Combien de bureaux de terrains / nationaux / régionaux sont actuellement opérationnels dans votre organisation ?	
Nombre d'employés (personnel international, personnel national, bénévoles, etc.)	
Combien de points focaux de sécurité travaillent actuellement avec vous ?	
Au niveau du siège, partagez-vous la responsabilité de la mise en œuvre du cadre de gestion des risques de sécurité ? Si oui, avec qui (fonction) ?	
CADRE DE GESTION DES RISQUES DE SÉCURITÉ	En place dans l'organisation (oui / non / en partie)
Les responsabilités décisionnelles en matière de gestion des risques de sécurité sont-elles clairement établies à tous les niveaux ?	
Votre organisation utilise-t-elle des informations sur le contexte de sécurité à d'autres fins telles que le plaidoyer, la communication avec les donateurs et/ou la programmation ?	
GESTION DES INCIDENTS ET DES CRISES	
L'organisation a-t-elle une politique de gestion des incidents / crises ?	
Existe-t-il un cadre de gestion des incidents au niveau du terrain / pays (procédures) ?	
Existe-t-il un cadre de gestion des incidents au niveau du siège (procédures) ?	
Le cadre de gestion des incidents inclut-t-il un arbre de communication ?	
Le cadre de gestion des incidents traite-t-il les incidents évités de justesse ?	
Formez-vous votre personnel à la gestion des incidents et/ou des crises et effectuez-vous des simulations ?	
L'organisation utilise-t-elle un système de gestion des incidents en ligne ?	

L'organisation utilise-t-elle un logiciel de traitement de texte ou un tableur comme base de son système de gestion des incidents ?	
Existe-t-il une procédure de communication sur les incidents convenue avec la compagnie d'assurance de l'organisation ?	
Existe-t-il un lien entre la politique de gestion des risques de sécurité et la politique RH de votre organisation ?	
COLLECTE D'INFORMATIONS SUR L'INCIDENT	
Avez-vous une définition organisationnelle du terme 'incident' ?	
Votre organisation utilise-t-elle des catégories définies pour décrire différents types d'incidents ? Si oui, sont-elles standardisées avec les catégories utilisées par les autres ONG avec lesquelles vous êtes partenaire ?	
Existe-t-il un modèle de rapport d'incident au niveau du terrain / national ? Si oui, a-t-il été standardisé avec d'autres ONG avec lesquelles vous êtes partenaire ?	
Existe-t-il une procédure de débriefing émotionnel (désamorçage) sur le terrain ?	
Existe-t-il une procédure de débriefing factuel sur le terrain ?	
Existe-t-il un système de stockage sécurisé pour les informations collectées sur le terrain ?	
Existe-t-il un système de stockage sécurisé pour les informations collectées au niveau national / régional ?	
Existe-t-il un système de stockage sécurisé pour les informations collectées au niveau du siège ?	
Votre organisation collecte-t-elle des informations sur les incidents externes (c'est-à-dire ceux qui n'ont pas d'impact sur votre organisation) ?	
RAPPORT ET ENREGISTREMENT DE L'INFORMATION SUR L'INCIDENT	
Existe-t-il une procédure pour signaler les incidents ?	
Existe-t-il des lignes directrices pour le modèle de rapport d'incident ?	
Existe-t-il un arbre de communication clair pour chaque bureau terrain ?	
Y a-t-il une liste de contacts disponibles au niveau du terrain / pays ?	
Existe-t-il un système d'enregistrement des incidents au niveau du terrain / pays ?	
Existe-t-il un système d'enregistrement des incidents au niveau régional ?	
Existe-t-il un système d'enregistrement des incidents au niveau du siège ?	
Consignez-vous les pertes et les dommages sur l'infrastructure ou les équipements ?	

Enregistrez-vous les menaces orales, écrites et cybernétiques dans votre organisation ?	
Enregistrez-vous les obstacles administratifs ?	
Consignez-vous la violence sexuelle (y compris le harcèlement) ?	
Les incidents associés à la violence sexuelle sont-ils signalés à l'aide du cadre de gestion régulière des incidents ?	
Est-ce que vous enregistrez les incidents évités de justesse ?	
Le système est-il sûr à tous les niveaux ? Les données sont-elles sécurisées ?	
ANALYSE DE L'INFORMATION ISSUE DE L'INCIDENT	
Existe-t-il un deuxième modèle de rapport d'incident fournissant des indications sur les informations à collecter à des fins d'analyse (par exemple, 72 heures après l'événement) ?	
Est-ce que quelqu'un au niveau du terrain / pays est responsable de l'analyse d'un incident ?	
Est-ce que quelqu'un au niveau régional est en charge de l'analyse d'un incident ?	
Est-ce que quelqu'un au niveau du siège fournit une analyse / vérification des résultats de l'analyse régionale et de terrain / pays ?	
Formez-vous votre personnel pour améliorer ses compétences analytiques ? (pas nécessairement et uniquement sur des sujets liés à la sécurité)	
Existe-t-il un système en place au niveau des pays pour cartographier (par exemple via une feuille de calcul) et analyser les incidents ?	
Existe-t-il une consultation des ressources externes (parties prenantes ou informations) pendant l'analyse, au niveau du terrain / pays ?	
Existe-t-il une consultation des ressources externes (parties prenantes ou informations) pendant l'analyse, au niveau régional ?	
Existe-t-il une consultation des ressources externes (parties prenantes ou informations) pendant l'analyse, au niveau du siège ?	
PARTAGE DE L'INFORMATION ISSUE DE L'INCIDENT	
Existe-t-il une ligne directrice ou une politique générale de « classification de l'information » dans l'organisation ?	
Existe-t-il une politique de communication interne au niveau du terrain / pays ?	
Existe-t-il une politique de communication interne au niveau régional ?	
Existe-t-il une politique de communication interne au niveau du siège ?	
L'organisation fait-elle partie d'un groupe de sécurité d'ONG sur le terrain / pays ? (exemples)	

L'organisation fait-elle partie d'un groupe de sécurité d'ONG au niveau régional ? (exemples)	
L'organisation fait-elle partie d'un groupe de sécurité d'ONG au niveau du siège ? (exemples)	
Existe-t-il une politique de communication externe au niveau du terrain / pays ?	
Existe-t-il une politique de communication externe au niveau régional ?	
Existe-t-il une politique de communication externe au niveau du siège ?	
L'organisation utilise-t-elle les réseaux sociaux pour la communication générale ?	
L'organisation a-t-elle établi des liens avec les medias ?	
L'organisation dispose-t-elle d'un système de cartographie des acteurs au niveau du terrain / pays ?	
L'organisation dispose-t-elle d'un système de cartographie des acteurs au niveau régional ?	
L'organisation dispose-t-elle d'un système de cartographie des acteurs au niveau du siège ?	
La tradition de la communication interne est-elle orale / écrite ?	
La tradition de la communication externe est-elle orale / écrite ?	
Existe-t-il un document de passation pour les points focaux de sécurité sur le terrain contenant des informations sur les incidents ?	
Le personnel est-il formé au partage d'informations sur les incidents et sur les politiques organisationnelles ?	
Les dirigeants et les membres du conseil d'administration bénéficient-ils de ce partage d'information ?	
UTILISATION DE L'INFORMATION ISSUE DE L'INCIDENT	
Y a-t-il une personne identifiée au niveau du terrain / pays en charge des actions de suivi (à mi-parcours) ?	
Existe-t-il une communication de suivi 1 mois après l'incident (les niveaux peuvent varier) ?	
Existe-t-il une communication de suivi 3 mois après l'incident (les niveaux peuvent varier) ?	
Existe-t-il un suivi de la mise en œuvre par le siège des leçons apprises ?	
Votre organisation effectue-t-elle une analyse quantitative ?	
Votre organisation effectue-t-elle une analyse qualitative ?	
Existe-t-il un système au niveau national pour effectuer une analyse quantitative des données sur les incidents ?	

Existe-t-il un système au niveau du siège pour effectuer une analyse quantitative des incidents ?	
Y a-t-il des réunions sur le terrain pour présenter les tendances en matière de données au personnel ?	
Y a-t-il des réunions au niveau national pour présenter les tendances en matière de données au personnel ?	
Y a-t-il des réunions au niveau régional pour présenter les tendances en matière de données au personnel ?	
Y a-t-il des réunions au niveau du siège pour présenter les tendances en matière de données au personnel?	
Les PFS de terrain / pays sont-ils consultés par les personnels du programme ?	
Le conseiller / responsable de la sécurité du siège est-il consulté par les personnels du programme ?	
Les membres de l'exécutif et du conseil d'administration sont-ils inclus dans l'analyse (par exemple l'analyse des tendances) ?	
Les informations sur les tendances en matière de données sont-elles partagées avec les parties prenantes externes ?	
Les tendances en matière de données de votre propre organisation sont-elles utilisées dans le plaidoyer ?	

OUTIL 2 : TYPOLOGIE DES INCIDENTS

Les définitions suivantes des différents types d'incidents sont données à titre indicatif. Les organisations n'ont pas besoin d'utiliser toutes les catégories dans leur gestion de l'information issue des incidents de sécurité. Cependant, elles sont encouragées à utiliser les définitions standards proposées pour faciliter l'échange de données et les comparaisons inter-organisations.

Les incidents sont définis en catégories (accident, action de l'autorité, crime, etc.) et sous-catégories associées. Les organisations peuvent choisir d'utiliser uniquement les catégories, les sous-catégories sélectionnées ou combinées.

Les catégories générales remplissent des fonctions différentes. Certaines regroupent les impacts sur l'événement (par exemple, décès ou dommages), d'autres la nature de l'événement (par exemple, la violence sexuelle), tandis que d'autres incluent des informations sur l'auteur de l'acte, en plus de décrire la nature de l'événement (par exemple, action criminelle ou d'autorité). D'autres incluent le contexte dans lequel l'événement s'est produit (par exemple l'insécurité générale) alors que d'autres catégories décrivent les moyens (par exemple l'utilisation d'armes). D'autres classifient la réponse de l'organisation.

C'est en fonction de l'analyse voulue que l'on utilise la catégorie la plus appropriée. Un seul événement peut être considéré à partir d'une variété de perspectives.

Pour la plupart des événements, plus d'une des catégories générales sont pertinentes. Les sous-catégories peuvent être traitées comme mutuellement exclusives, ce qui signifie qu'une seule des sous-catégories s'applique.

Voir aussi la définition des catégories d'événements utilisées dans l'analyse des tendances de Insecurity Insight et les données sur Humanitarian Data Exchange.

CATÉGORIES	SOUS CATÉGORIES	DÉFINITION
Accident Maladie Catastrophe naturelle Tout accident de la route impliquant des membres du personnel ou des véhicules de l'organisation et d'autres incidents non Intentionnels, les accidents, catastrophes ou maladies soudaines.	**Accident : Décès**	Tout décès involontaire qui ne peut être attribué à des causes naturelles. Les causes de décès accidentel peuvent inclure des accidents de véhicules, des blessures graves, etc.
	Accident : Autre	Un incident aléatoire qui entraîne des dommages au personnel et/ou des dommages sur les biens de l'organisation.
	Accident : Véhicule	Un accident impliquant le véhicule d'une organisation. Véhicule désigne toute forme de transport, y compris, mais sans s'y limiter, les voitures, les camions, les autobus, les mobylettes, etc.
	Accident : Incendie	Tout incendie involontaire ou de cause naturelle endommageant la propriété ou mettant en danger le personnel. Cela peut inclure les incendies de forêt ou les incendies accidentels (tels que les incendies électriques ou les fuites de gaz), etc.
	Maladie	Toute maladie grave d'un employé.
	Catastrophe Naturelle	Catastrophe naturelle qui survient ou est prévue dans une ville ou un pays où l'organisation a un bureau. Les catastrophes naturelles peuvent inclure les tremblements de terre, les éruptions volcaniques, les ouragans, les tornades, les dégâts provoqués des tempêtes (grêle, inondations soudaines, etc.), les inondations, les tsunamis, etc.
Action de l'autorité (AA) Actions directes ou indirectes prises par un acteur étatique ou non étatique qui entrave la livraison de l'aide.	**AA : Abus de pouvoir**	L'utilisation de pouvoirs législatifs, exécutifs ou autres autorisés par des représentants du gouvernement pour des gains privés illégitimes. L'acte illégal d'un fonctionnaire ne constitue un abus de pouvoir que si l'acte est directement lié à ses fonctions officielles.
	AA : Accès refusé	Actes qui : a) empêchent une organisation d'atteindre les bénéficiaires ou les bénéficiaires potentiels pour l'évaluation des besoins ou la fourniture directe de services b) empêchent les bénéficiaires d'accéder aux services fournis par une organisation.
	AA : Accusations	Une accusation de la part des autorités du pays d'accueil d'actes répréhensibles.
	AA : Application des lois	Application de lois, de décrets, ou de règlements existants ou nouveaux qui, lorsqu'ils sont appliqués, ont un effet réel sur la livraison de l'aide. Cela peut inclure la confiscation de matériel, mettre des personnes / organisations sur des listes de surveillance, etc.
	AA : Arrestation (Voir aussi Accusations, détentions et emprisonnements)	Arrestations de personnel. Ceux qui procèdent à l'arrestation doivent exercer des fonctions gouvernementales (comme la police) afin de différencier cet incident d'un incident de prise d'otages. Les arrestations suivent généralement des accusations formelles.
	AA : Poursuites judiciaires	Accusation légale formelle faite par une autorité gouvernementale affirmant qu'un membre du personnel ou l'organisation a commis un crime.

CATÉGORIES	SOUS CATÉGORIES	DÉFINITION
Authority action (AA) Actions directes ou indirectes prises par un acteur étatique ou non étatique qui entrave la livraison de l'aide.	**AA : Checkpoint**	Un poste de contrôle non frontalier ou frontalier érigé dans des zones contrôlées par des militaires, des paramilitaires ou des groupes armés afin de surveiller ou de contrôler les mouvements de personnes et de matériel ayant une incidence sur la fourniture de l'aide.
	AA : Refus de visa	Retarder ou refuser un timbre officiel, un visa ou tout autre permis autorisant l'entrée dans un pays ou un territoire d'un pays requis pour livrer une aide.
	AA : Détention	Garder un membre du personnel en détention avant les accusations officielles ou sans aucune charge officielle; comprend la détention temporaire pendant des heures ou des jours.
	AA : Expulsion	Acte de forcer un membre du personnel ou une organisation à quitter un pays ou un territoire.
	AA : Amende	Somme d'argent qui doit être payée par l'organisation parce qu'elle n'a pas respecté une règle ou une loi.
	AA : Fermeture forcée	Ordre du gouvernement ou d'autres autorités d'arrêter les opérations dans un pays ou un territoire ; inclut la fermeture affectant seulement un ou plusieurs programmes.
	AA : Action gouvernementale	Action du gouvernement hôte ou donateur qui a un impact direct ou indirect sur la capacité financière d'une organisation à fournir de l'aide ; comprend le gel des fonds, l'introduction de taxes ou la suppression des subventions.
	AA : Emprisonnement	Détention d'un membre du personnel dans un lieu officiel connu ou inconnu, comme une prison, souvent suite à des accusations formelles.
	AA : Introduction de lois	Fait référence à la rédaction ou au vote des lois, décrets ou règlements qui, lorsqu'ils sont appliqués, auront un effet potentiel ou réel sur la livraison de l'aide. Cela peut inclure, mais sans s'y limiter, des procédures d'enregistrement restrictives, des règles d'importation, ou la divulgation régulière de sources financières.
	AA : Enquête	Le processus ou l'acte d'examiner les faits liés aux allégations contre les membres du personnel ou de l'organisation.
	AA : Perquisition	Perquisition des locaux de l'organisation par les autorités.
Crime Incidents criminels ayant une incidence sur les biens d'une organisation ou sur un membre du personnel.	**Crime : Vol à main armée**	Un vol à main armée ou dans lequel les auteurs du vol portent des armes à feu qui ont affecté des employés ou des biens
	Crime : Incendie criminel	Tout incendie volontaire mettant en danger la vie des employés ou endommageant des biens. Les incendies criminels comprennent, mais sans s'y limiter, l'utilisation de dispositifs incendiaires, le sabotage intentionnel de systèmes électriques ou de conduites / réservoirs de gaz, et l'utilisation d'un accélérateur pour détruire les biens.

CATÉGORIES	SOUS CATÉGORIES	DÉFINITION
Crime Incidents criminels ayant une incidence sur les biens d'une organisation ou sur un membre du personnel.	**Crime : Chantage**	Les menaces, l'extorsion ou la manipulation d'une personne pour l'obliger à faire quelque chose ; y compris à donner quelque chose, en particulier de l'argent, par la force ou la menace.
	Crime : Cambriolage	L'acte de pénétrer illégalement dans les locaux ou les véhicules de l'organisation, avec l'intention de voler.
	Crime : Vol avec infraction	S'introduire dans une résidence, généralement avec l'intention de voler. Utiliser uniquement si les personnes dormaient ou ne se sont pas rendu compte du cambriolage.
	Crime : Braquage / Détournement de véhicule	Tout incident dans lequel un véhicule contenant un employé (s) ou appartenant à l'organisation est saisi de force.
	Crime : Cyber attaque	Exploitation délibérée de systèmes informatiques, et de réseaux tributaires de la technologie perturbant et pouvant compromettre les données et mener à la cybercriminalité.
	Crime : Fraude	Acte trompeur ou criminel en vue d'obtenir un gain financier ou personnel.
	Crime : Intrusion	Fait de s'introduire dans les locaux d'une organisation, ses véhicules ou ses résidences sans y être invité, par des criminels ou des civils (mais pas par les autorités de l'État).
	Crime : Pillage	Vol pendant les troubles, la violence, les émeutes ou d'autres bouleversements.
	Crime : Piraterie	Attaquer et voler des navires en mer ou des bateaux sur les rivières.
	Crime : Vol qualifié	Événements dans lesquels a) l'agresseur n'était pas armé, b) le membre du personnel était présent pendant l'incident et est parfaitement conscient d'avoir été volé, et c) des biens ont été pris.
	Crime : Vol de biens	Toute situation dans laquelle des biens personnels sont volés à un employé ou dans un lieu sans que la victime ne s'en aperçoive.
	Crime : Vol de biens de l'organisation	Toute situation dans laquelle un bien de l'organisation (au-delà d'une valeur prédéfinie) est volé sans qu'un membre du personnel ne s'en aperçoive.
	Crime : Vandalisme	Destruction ou endommagement délibéré des biens de l'organisation ou de son personnel. Dégâts matériels.
Dégradation Toute dégradation des biens de l'organisation.	**Dégâts matériels**	Toute dégradation ou détérioration matériels, au-delà d'un montant prédéfini, involontaire (par exemple, catastrophes naturelles, accidents, etc.) ou intentionnelle (par exemple, les émeutes qui causent des dommages matériels, etc.) sur les biens de l'organisation.

CATÉGORIES	SOUS CATÉGORIES	DÉFINITION
Mort Tout décès de membres du personnel pour une cause quelconque	**Décès : Accident**	(Voir Accident)
	Décès : Intentionnel (homicide)	(Voir TBK)
	Décès : Naturel	Tout décès pouvant être attribué à une cause naturelle, telle qu'une crise cardiaque, une maladie ou un accident vasculaire cérébral.
	Décès : Suicide	La mort volontaire et intentionnelle d'un employé. Le suicide est défini comme la prise volontaire et intentionnelle de sa propre vie.
Insécurité générale (IG) Les incidents liés au contexte qui créent de l'insécurité et affectent directement ou indirectement la livraison de l'aide. Affecte ou non directement l'agence, son personnel ou son infrastructure.	**IG : Activité armée**	Actions armées d'un État, une entité non étatique ou une entité armée organisée.
	IG : Attaque sur une autre organisation	Attaque sur une autre organisation qui n'a pas directement affecté l'agence.
	IG : Coup d'Etat	Coups d'Etat, mutinerie et autres rébellions de la part de toute force armée. Un coup d'Etat est défini comme une tentative (généralement armée), réussie ou non, violente ou non, de remplacer un gouvernement. Une tentative de coup d'Etat peut être politiquement déstabilisante.
	IG : Tirs croisés / combats actifs	Toute situation dans laquelle un employé ou un bien de l'organisation est pris dans une attaque ou un échange de tirs entre deux ou plusieurs groupes armés. Dans cette situation, les employés impliqués et les biens ne sont pas la cible de l'attaque.
	IG : Manifestation	Toute manifestation (y compris les contestations, marches, sit-in, piquets de grève, etc.) qui est non-violente. Rassemblement de masse de personnes à des fins politiques ou sociales.
	IG : Fusillade	Tirs délibérés sur des personnes autres que le personnel de l'organisation (voir aussi TBK : homicide et UA : armes à feu).
	IG : La grève / non présentation	Décision délibérée du personnel de ne pas venir travailler pour des raisons autres que médicale.
	IG : Troubles	Agitation civile ou politique, ainsi que les comportements assimilés à ceux d'une foule ou présentés comme tumultueux. Ces comportements incluent le pillage, les soulèvements en prison, mise à feu par la foule de différents biens, les combats avec la police (et généralement les manifestants).
Tué, blessé ou kidnappé (TBK) : Tout incident entraînant la mort, les blessures ou l'enlèvement d'un membre du personnel. Généralement les événements critiques.	**TBK : Rapt / détournement / prise d'otage / enlèvement**	Tout incident dans lequel le personnel est saisi de force. Cet incident peut ou non impliquer une demande de rançon.
	TBK : Battu	Incident dans lequel un membre du personnel a été agressé, à coups de poings ou pieds ou avec des objets (bâtons ou objets contondants).
	TBK : Décès : Intentionnel (homicide) / assassiné	Tout décès intentionnellement causé, par exemple, par balle, attaque physique, empoisonnement, etc. Les morts intentionnelles n'incluent pas les suicides.

CATÉGORIES	SOUS CATÉGORIES	DÉFINITION
Tué, blessé ou kidnappé (TBK) : Tout incident entraînant la mort, les blessures ou l'enlèvement d'un membre du personnel. Généralement les événements critiques.	**TBK : Disparu**	Incident dans lequel un membre du personnel a disparu ou est porté disparu. Distinction entre la disparition et les enlèvements : a) par acteur : les acteurs non étatiques ont tendance à enlever les personnes alors que les acteurs étatiques ont tendance à les faire « disparaître ». Elles deviennent alors des personnes « disparues » ; b) par la communication des auteurs de l'enlèvement du personnel : les ravisseurs ont tendance à faire des demandes (par exemple, une rançon) alors que l'on n'a plus de nouvelles personnes enlevées et des personnes disparues. c) par motif : les enlèvements tendent à répondre à une demande spécifique tandis que les disparitions tendent à être effectuées pour faire taire un membre du personnel, souvent pour des raisons politiques.
	TBK : Torture	Mutilation physique intentionnelle / blessure qui est explicitement qualifiée de torture du personnel.
	TBK : Blessés	Incident dans lequel un membre du personnel a été blessé. La plupart des blessures dans cette catégorie sont causées par des armes, en opposition à la sous-catégorie « battu ».
Motif Classification du motif de(s) l'auteur (s).	**Motif : Attaque**	Attaques ciblant directement l'organisation.
	Motif : Mauvais endroit, mauvais moment	Attaques non dirigées contre l'organisation ou son personnel mais dans lesquelles les membres du personnel ou des biens de l'organisation ont été affectés parce qu'ils se trouvaient près d'une attaque générale ou d'une attaque ciblée contre une autre entité ou individu.
Evité de Justesse (EJ) Les incidents qui auraient pu causer un préjudice ou affecter la livraison de l'aide. Comprend toute situation dans laquelle un incident de sécurité est survenu mais ne s'est pas produit, a eu lieu près d'un travailleur humanitaire / d'une organisation / d'un programme, ou lorsque les personnes impliquées ont pu éviter tout dommage grave. (S'il y a des dommages, l'événement est inclus dans la sous-catégorie sous TBK).	**EJ : Crime**	L'incident évité de justesse s'est produit dans le contexte d'un événement criminel.
	EJ : Armes explosives	L'incident évité de justesse s'est produit dans le cadre de la détonation d'une arme explosive (par exemple, un bombardement d'un bâtiment voisin ou un attentat à la bombe dans un restaurant fréquenté par des membres du personnel de l'organisation). Il s'agit des événements spécifiques par opposition ceux d'utilisation générale d'armes explosives dans un environnement non sécurisé.
	EJ : TBK	L'incident a évité de justesse qu'un membre du personnel ne soit tué, blessé ou kidnappé.

CATÉGORIES	SOUS CATÉGORIES	DÉFINITION
Mesures de sécurité (MS) Actions entreprises par les organisations en réponse à l'insécurité généralisée ou à un incident de sécurité.	**MS : Evacuation : médicale**	Evacuation d'un employé pour des raisons médicales, généralement à cause des blessures ou d'une maladie qui ne peuvent pas être traitées de manière adéquate à l'hôpital local, au cabinet du médecin ou au centre de traitement.
	MS : Evacuation : non-médicale	Evacuation d'un employé pour des raisons de sécurité. Notez que l'évacuation fait référence au retrait du personnel du pays d'opération. Le déplacement du personnel vers un autre endroit du pays pour des raisons de sécurité est appelé relocalisation.
	MS : Hibernation	Fait de rester à l'abri jusqu'à ce que le danger soit passé ou qu'une aide supplémentaire soit fournie.
	MS : Couvre-feu imposé	Imposition d'un couvre-feu dans une ville ou un pays où l'organisation a un bureau.
	MS : Fermeture de bureau	Décision de fermer un bureau en réponse au contexte général de sécurité ou à un événement spécifique.
	MS : Surveillance constante	Suivi actif d'une situation de sécurité en vue de potentiellement changer les mesures de sécurité.
	MS : Suspension du programme	Modification importante du programme en arrêtant une activité ou un projet spécifique.
	MS : Déménagement	Déplacement du personnel vers une autre ville ou bureau dans le pays d'opération pour des raisons de sécurité.
	MS : Déplacement restreint, pas de couvre-feu	Toute restriction de déplacement affectant le personnel. Ce type d'événement est semblable à une alerte et peut être le résultat d'une agitation politique ou sociale, d'une épidémie ou d'une catastrophe naturelle.
Violence sexuelle Tout incident dans lequel un membre du personnel a subi une forme quelconque de violence sexuelle.	**Violence sexuelle : comportement sexuel agressif**	Comportement potentiellement violent axé sur des pulsions sexuelles gratifiantes.
	Violence sexuelle : tentative d'agression sexuelle	Tentative de contact sexuel sur le corps d'une autre personne sans son consentement.
	Violence sexuelle : viol	Rapports sexuels (pénétration orale, vaginale ou anale) contre la volonté et sans le consentement de la personne.
	Violence sexuelle : agression sexuelle	Acte de contact sexuel sur le corps d'une autre personne sans son consentement.
	Violence sexuelle : commentaires sexuels non désirés	Avances verbales qui comprennent siffler, crier, et/ou dire des phrases sexuelles, façon explicites ou implicite ou qui ne sont pas souhaitées.
	Violence sexuelle : attouchements sexuels non désirés	Toucher, d'une nature sexuelle non désirée indépendamment de l'intensité du toucher, d'une façon sexuelle non souhaitée. Cela peut inclure masser, tâter, s'accaparer toute partie du corps d'une autre personne.

CATÉGORIES	SOUS CATÉGORIES	DÉFINITION
Violence sexuelle Tout incident dans lequel un membre du personnel a subi une forme quelconque de violence sexuelle.	**Violence sexuelle : harcèlement sexuel**	Toucher, d'une nature sexuelle non désirée indépendamment de l'intensité du toucher, d'une façon sexuelle non souhaitée. Cela peut inclure masser, tâter, s'accaparer toute partie du corps d'une autre personne. Avances sexuelles importunes, demandes de faveurs sexuelles et autres comportements verbaux ou physiques à caractère sexuel qui ont un impact sur l'emploi de la personne ciblée. Par exemple: a) la soumission à un tel comportement est explicitement ou implicitement la condition pour qu'une personne garde son emploi, ou b) la soumission ou le rejet d'un tel comportement est utilisé contre la personne, ou c) un tel comportement a pour objet ou pour effet d'interférer déraisonnablement avec la performance au travail d'une personne ou de créer un environnement de travail intimidant, hostile ou offensant.
Menace Menace(s) directe(s) ou indirecte(s) faite(s) par un acteur étatique ou non étatique qui entravent la livraison de l'aide.	**Menace : harcèlement en personne**	Événements dans lesquels un membre du personnel est directement harcelé par une personne ou un groupe de personnes (par exemple, le harcèlement sur les activités ou du programme de l'organisation).
	Menace : intimidation en personne	Evénements dans lesquels un membre du personnel est directement intimidé par une personne ou un groupe de personnes (par exemple, un membre du personnel s'est senti intimidé par des acteurs armés patrouillant près d'une distribution de nourriture).
	Menace : menaces en personne	Evénements dans lesquels un membre du personnel est directement menacé par une personne ou un groupe de personnes; devrait inclure une certaine forme de conséquence en cas de non-conformité (par exemple, une menace de représailles pour ne pas inclure une personne dans une activité de l'organisation).
	Menace : menaces à distance contre l'organisation	Événements dans lesquels l'organisation ou un membre du personnel est menacé pas en personne mais par un mécanisme distant (par exemple, courrier électronique, SMS, téléphone ou via des menaces générales diffusées sur un site Web ou sur les réseaux sociaux (Twitter, Facebook). Inclure les menaces directes lancées par les civils lors des manifestations.
	Menace : risque de réputation	Événements impliquant un risque perçu, réel ou potentiel pour le logo / l'emblème, l'image ou la réputation de l'organisation.
	Menace : menace de fermeture	Événements impliquant la menace d'une fermeture forcée d'une activité, d'un programme ou d'une organisation.
	Menace : Témoin	Événements dans lesquels un membre du personnel est témoin d'une attaque ou d'un crime contre un autre membre du personnel, des membres de la famille ou des bénéficiaires.

CATÉGORIES	SOUS CATÉGORIES	DÉFINITION
Utilisation d'armes (UA) Actes incluant le type d'arme qui a été utilisé dans l'incident, ce qui a affecté le personnel, l'infrastructure ou la livraison de l'aide.	**UA : Explosifs : Bombes aériennes**	Armes explosives larguées par voie aérienne, y compris les armes incendiaires, à l'exclusion des bombes à sous-munitions et des missiles sol-sol.
	UA : Explosifs : Bombes à fragmentation	Armes explosives larguées ou lancées au sol éjectant des sous-munitions plus petites.
	UA : Explosifs : Grenades à main	Petit engin explosif lancé à la main, conçu pour exploser après un impact ou après un certain temps.
	UA : Explosifs : Mines	Toute explosion de mine impliquant du personnel.
	UA : Explosifs : Autres	Toute autre arme explosive non répertoriée ou une combinaison des éléments ci-dessus.
	UA : Explosifs : RCIED	Un engin explosif improvisé télécommandé, tel qu'une bombe, aurait été laissé sur le bord de la route et aurait explosé lorsque la cible serait proche.
	UA : Explosifs : Sol-sol	Comprend des missiles, des mortiers ou des obus lancés à partir d'un système de lancement mobile ou stationnaire, y compris des grenades propulsées par fusée.
	UA : Explosifs : SVIED	Explosif improvisé par une ou des personne(s), par ceinture explosive ou explosive dans un sac à dos.
	UA : Explosifs : VBIED	Dispositif explosif improvisé transporté par un véhicule, par voiture piégée, ou une voiture contenant un engin explosif.
	UA : Biologique	Toute utilisation d'armes biologiques dans une ville ou un pays dans lequel l'organisation a un bureau.
	UA : Chimique	Toute utilisation d'armes chimiques dans une ville ou un pays dans lequel l'organisation a un bureau.
	UA : Nucléaire	Toute utilisation d'armes nucléaires, explosives ou non, dans une ville ou un pays où l'organisation a un bureau.
	UA : Radiologique	Toute utilisation d'armes radiologiques, communément appelées « bombes sales », dans une ville ou un pays où l'organisation a un bureau. Les incidents possibles impliquant des armes radiologiques vont des attaques contre des centrales nucléaires aux attaques de dispositifs nucléaires improvisés qui pourraient être construits à partir de matériaux radiologiques volés.
	UA : Armes à feu légères	Toute utilisation d'armes à feu ou d'armes de poing impliquant des employés ou des biens de l'organisation.

CATÉGORIES	SOUS CATÉGORIES	DÉFINITION
Occupation	**Occupation des bureaux de l'organisation**	La saisie et l'occupation de tout bâtiment, entrepôt ou complexe immobilier d'organisations par des agents civils ou gouvernementaux.
Autres	**Autre incident**	Un incident qui ne peut pas être décrit correctement par l'une des catégories d'incidents prédéfinies dans cette liste. Notez que si cette catégorie est sélectionnée, le rapporteur doit fournir une description complète de l'incident dans le champ 'Description de l'incident'.

OUTIL 3 : INCIDENT ORGANISATIONNEL OU EXTERNE

Les organisations se concentrent souvent sur le signalement et l'enregistrement des incidents organisationnels (incidents ayant un impact sur l'organisation, son personnel, ses biens et sa réputation) et non sur les incidents externes (incidents ayant un impact sur d'autres organisations). L'organisation doit définir ce qui constitue un incident affectant l'organisation et décider si les incidents externes doivent également être signalés et enregistrés.

Voici un exemple de grille élaborée par une organisation pour aider à évaluer ce qui serait considéré comme un incident organisationnel et ce qui ne le serait pas. Ce qui suit peut faire l'objet d'adaptations et de modifications, en fonction de la politique et des procédures de sécurité d'une organisation. Veuillez trouver une version vierge ci-dessous.

PERSONNE IMPLIQUÉE	HEURES DE TRAVAIL		IMPACT SUR LES BIENS DE L'ORGANISATION		QUALIFICATION
	Oui	Non	Oui	Non	
Le personnel n'est pas originaire du pays d'origine (affectation internationale)	X		X		Incident organisationnel
	X			X	Incident organisationnel
		X	X		Incident organisationnel
		X		X	Si pas de violence : Non Si avec violence : Oui
Le personnel est originaire du pays	X		X		Incident organisationnel
	X			X	Incident organisationnel
		X	X		Incident organisationnel
		X		X	Incident non organisationnel
Partie prenante externe contractée par l'organisation	X		X		Incident organisationnel
	X			X	Incident non organisationnel
		X	X		Dépend du type d'incident ou de biens et de l'impact de l'incident : oui ou non
		X		X	Incident non organisationnel

Pour votre organisation, utilisez :

PERSONNE IMPLIQUÉE	HEURES DE TRAVAIL		IMPACT SUR LES BIENS DE L'ORGANISATION		QUALIFICATION
	Oui	Non	Oui	Non	
Le personnel n'est pas originaire du pays d'origine (affectation internationale)					
Le personnel est originaire du pays					
Partie prenante externe contractée par l'organisation					

OUTIL 4 : MODÈLE DE RAPPORT D'INCIDENT

Ce modèle examine les informations les plus immédiates nécessaires à la gestion des incidents de sécurité et à l'analyse préliminaire.

COORDONNÉES DE L'AUTEUR :	
Fiabilité de la source et estimation de la validité de l'information[37] (selon la grille d'analyse approuvée) :	

1. COORDONNÉES DE L'AUTEUR DU RAPPORT	
Auteur du rapport :	Nom complet, poste (relation avec l'organisation si externe).
L'auteur du rapport est-il impliqué dans l'incident ?	Oui / Non
Date du rapport :	Date de soumission (et version du rapport si ce n'est pas la première version).
2. INFORMATION GÉNÉRALE SUR L'INCIDENT	
Localisation :	Détails exacts sur l'endroit de l'incident (y compris les coordonnées GPS si possible)
Date de l'incident :	Date de l'incident (si unique) ou séquence détaillée des incidents si plusieurs événements.
Heure de l'incident :	Moment exact de l'incident (si unique) ou séquence détaillée / calendrier des incidents si plusieurs événements (heure du jour / nuit).
Programme pays :	Détails exacts sur le(s) programme(s) d'ONG concerné(s).
3. CATÉGORISATION DE L'INCIDENT	
Type d'incident :	Intentionnel ou accidentel ; Interne à l'organisation ou externe ; Piratage ; vol ; extorsion ; accident de la circulation ; etc.

[37] Ce qui peut être indiqué au début de chaque rapport ou dans le rapport lui-même.

4. INDIQUER LA GRAVITÉ DE L'INCIDENT	
Evité de justesse :	Toute situation dans laquelle un incident de sécurité a failli survenir ou s'est produit à proximité d'un travailleur humanitaire / d'une organisation / d'un programme, ou lorsque les personnes concernées ont pu éviter tout dommage grave.
Non critique :	Les personnes n'ont pas été menacées physiquement et/ou psychologiquement. Aucune blessure.
Modéré :	Les personnes ont été menacées physiquement et/ou psychologiquement. Blessures mineures qui ne nécessitent pas de suivi médical prolongé.
Sérieux :	Blessures graves nécessitant un suivi médical prolongé. Menace grave pour l'intégrité physique et/ou psychologique.
Mortel :	Un membre du personnel de l'organisation est mort en conséquence directe de l'incident.
Encore inconnu :	

5. DESCRIPTION DE L'INCIDENT
Présentez brièvement mais précisément une description de l'événement.

6. VICTIME(S)	
Nom(s) complet(s) : Personnel national / international :	Veuillez indiquer si la victime est un membre du personnel national ou international. Quelle est leur nationalité ?
Genre :	Homme(s) ou Femme(s) ou Autre
Age :	Quel âge a la (les) victime(s) ?
Autres détails pertinents pour l'affaire :	La personne souffrait-elle d'un handicap ou d'une maladie qui aurait pu avoir un impact sur l'événement ?
Ancienneté et poste dans l'organisation :	Depuis combien de temps la personne travaille-t-elle sur ce programme ? Position / responsabilité de la victime au sein de l'organisation.
Etat actuel de la victime :	Indemne, blessé (préciser la gravité, physique ou psychologique) ou décédé.

7. TÉMOINS
Indiquez le(s) nom(s) complet(s) et les coordonnées personnelles des personnes présentes lorsque l'incident s'est produit et qui peuvent aider à clarifier les faits.

8. MESURES IMMÉDIATES PRISES À LA SUITE DE L'ACCIDENT	
Contacts internes :	Qui a été informé en interne de l'incident (programme / mission) ?
Contacts externes : *Bailleurs* *Autres organisations humanitaires / de développement :* *Médias :* *Autre :*	Quelles autorités externes (locales ou nationales, administratives et/ou judiciaires, militaires) ont été contactées suite à l'incident ?
Actions prises concernant les programmes :	L'incident a des conséquences pour le programme telles que la réduction du personnel ou la cessation des activités ou du programme dans son ensemble.
Mesures prises affectant le personnel impliqué :	Le suivi / débriefing / appui psychologique est / était nécessaire pour le personnel impliqué dans l'incident.
9. ANALYSE PRÉLIMINAIRE – RISQUE(S) POUR LE PROGRAMME	
Opérationnel :	Quelles mesures d'atténuation ont été prises ? Si l'incident implique de nouveaux risques ou augmente un risque préexistant pour les opérations de l'organisation, veuillez préciser.
Ressources humaines :	Quelles mesures d'atténuation ont été prises ? Si l'incident implique de nouveaux risques ou augmente un risque préexistant pour le personnel de l'organisation, veuillez préciser.
Financier / Matériel :	Quelles mesures d'atténuation ont été prises ? Si l'incident implique de nouveaux risques ou augmente un risque préexistant au niveau financier ou pour les propriétés de l'organisation, veuillez le préciser.
Légal / Réputation :	Quelles mesures d'atténuation ont été prises ? Si l'incident implique de nouveaux risques ou augmente un risque préexistant au niveau légal ou pour l'image de l'organisation, veuillez préciser.
Autres :	
10. SUPPORT DU SIÈGE	
Indiquez si un support du siège est nécessaire et si oui, de quel support s'agit-il ?	

OUTIL 5 : GRILLES D'ANALYSE DES INCIDENTS

Ces grilles vont guider l'analyse des impacts et des causes d'un incident, et la façon dont la gestion et le suivi ont été mis en œuvre pendant et après cette première analyse.

1. IDENTIFICATION DE L'IMPACT DE L'INCIDENT

Durée de l'incident	Combien de temps a duré l'incident ?
Type de contexte	Selon les catégorisations utilisées dans l'organisation du contexte et du type et niveau de violence.
Phase de sécurité	Tel que défini dans les documents de sécurité de l'organisation.
Estimation de la perte	
Organisation	
Argent	Indiquez quels ont été les coûts directs pour l'organisation à la suite de l'incident (chiffres).
Equipement	Indiquer si l'équipement / les biens ont été endommagés et leur valeur.
Documentation	Indiquer si des documents sensibles (par exemple, une liste de personnel) ou quelque chose utilisée pour authentifier des documents (par exemple, des tampons) sont manquants.
Autres	
Personnel	
Argent	Indiquez le montant d'argent perdu par le personnel pendant l'incident.
Equipement	Indiquer si des biens appartenant au personnel ont été endommagés pendant l'incident et leur valeur.
Documentation	Indiquer si des documents personnels appartenant au personnel sont manquants.
Autres	
Débriefing émotionnel	Indiquez si un débriefing émotionnel a été fait ou non. Spécifiez la date.

2. IDENTIFICATION DES CAUSES DE L'INCIDENT

FACTEURS CONTRIBUTIFS POTENTIELS (RÉPONSES MULTIPLES POSSIBLES)		
Type d'activités	L'incident est lié au type de travail de l'organisation.	Spécifier
Manque d'acceptance de notre programme	L'incident est le résultat du manque d'acceptance du programme.	Spécifier
Mesures de protection insuffisantes	L'incident est le résultat de l'absence de mesures de protection.	Spécifier
Non-respect des règles de sécurité et/ou des POS ?	L'incident est le résultat d'une non-conformité aux règles de sécurité et/ou aux procédures.	Spécifier
Insouciance / manque de vigilance	L'incident est le résultat de l'imprudence ou du manque de vigilance de l'équipe.	Spécifier
Manque d'équipement de communication	L'incident est le résultat du manque (absence ou dysfonctionnement) d'équipement de communication nécessaire à la sécurité et à la sûreté de l'équipe.	Spécifier
Conflit (s) au sein de l'équipe	L'incident est le résultat d'un conflit entre deux ou plusieurs membres de l'équipe.	Spécifier
Incompétence / conduite du véhicule non contrôlée	L'incident est le résultat du manque de capacité du conducteur à gérer le moyen de transport impliqué dans l'incident.	Spécifier
Comportement inapproprié	L'incident est le résultat du comportement inapproprié d'un ou plusieurs membres de l'équipe (violation du code de conduite, vêtements inappropriés, etc.).	Spécifier
Changement de contexte	L'incident est le résultat du changement de la situation globale (c'est-à-dire le contexte).	Spécifier
Conflit culturel externe	L'incident est le résultat de conflits préexistants au sein de la communauté tels que des confrontations ethniques ou religieuses.	Spécifier
Autre	Décrire le(s) facteur(s) non répertorié(s) pouvant avoir contribué à l'incident.	

3. IDENTIFICATION DU MOTIF ET ACTIONS POTENTIELLES

QUESTION/ PROCESSUS	RÉPONSE	IMPLICATION POTENTIELLE (BASÉE SUR L'ÉVALUATION)	ACTIONS POSSIBLES DE L'ORGANISATION
1. Est-ce que cet incident s'est déjà produit avant et à quel point était-ce similaire ?	Oui	Menace précise (attestée par des pièces justificatives)	Communiquer les évaluations de la menace, continuer à les utiliser comme base pour les décisions de sécurité
	Non	Menace non précise (attestée par des pièces justificatives)	Revoir l'évaluation de la menace et les mesures de sécurité basées sur celle-ci
	Non	Menace ancienne (mise en évidence par des pièces justificatives)	Revoir l'évaluation de la menace et les mesures de sécurité basées sur celle-ci
2. Si les procédures appropriées ont été suivies, quel a été le résultat ?	Positif	Les procédures appropriées ont été suivies	Renforcer les procédures
		Le personnel a eu de la chance	Reconsidérer les procédures
	Négatif	Pratiques de sécurité imparfaites	Reconsidérer les pratiques de sécurité
		Tendance à prendre des risques élevés	Communiquer au personnel Former / reformer le personnel
3. Si les procédures appropriées n'ont pas été suivies, quel a été le résultat ?	Positif	Procédures inappropriées	Reconsidérer les procédures ou leur applicabilité à toutes les situations
		Le personnel a eu de la chance	Reconsidérer les procédures
	Négatif	Manque de connaissance des procédures, éventuellement pour les raisons suivantes : • Pas de briefing de sécurité pour le nouveau personnel ; • Absence d'un plan de sécurité (POS et plans d'urgence) ; • Une attention insuffisante à fournir au personnel des séances d'information sur la sécurité et l'accès au plan de sécurité ; • Manque de temps et d'encouragement pour le personnel à lire le plan de sécurité.	Considérer une façon de mieux communiquer avec le personnel
		Échec des tentatives de suivi des procédures, éventuellement pour les raisons suivantes : • Les procédures sont trop compliquées à retenir et à suivre ; • Nécessite une formation qui n'a pas été fournie ; • Nécessite un équipement qui n'est pas toujours disponible ou qui fonctionne.	Reconsidérer les procédures, la formation, la disponibilité de l'équipement

QUESTION/ PROCESSUS	RÉPONSE	IMPLICATION POTENTIELLE (BASÉE SUR L'ÉVALUATION)	ACTIONS POSSIBLES DE L'ORGANISATION
3. Si les procédures appropriées n'ont pas été suivies, quel a été le résultat ?	Négatif	Le personnel n'est pas d'accord avec les procédures, peut-être pour les raisons suivantes : • Des procédures inappropriées ; • Nécessité d'une formation plus poussée pour convaincre le personnel de l'importance des procédures ; • Pratiques d'embauche inappropriées ; • Un manque de mise en œuvre des procédures au sein de l'organisation.	Reconsidérer les pratiques appropriées en matière de sécurité

4. ANALYSE DE LA GESTION DE L'INCIDENT

Rendre compte aux responsables de programme	Avec quel succès l'information a-t-elle été transmise ? Les délais de l'organisation ont-ils été respectés ?
Arbre de communication	Dans quelle mesure la transmission de l'information dans l'ensemble du site a-t-elle été efficace ? L'arborescence des communications a-t-elle fonctionné correctement ?
Rôles et responsabilités	Les responsables savaient-ils quoi faire en fonction de leurs responsabilités et de leurs tâches ?
Pré-identification des personnes-ressources clés avant l'incident	Avons-nous clairement identifié des personnes clés (externes et internes) qui nous ont aidés dans la gestion de l'incident ? Avons-nous essayé de contacter une institution / autorité pour nous aider ? Avons-nous identifié la ou les personnes-ressources clés ? Indiquez cette personne de contact.
Communication Siège – Terrain – Siège	Comment était la communication entre le siège et le terrain ? De quoi avons-nous besoin pour nous améliorer ?
Autre	

OUTIL 6 : COMMENT EFFECTUER UN DEBRIEFING FACTUEL

Le processus de débriefing factuel devrait commencer après l'organisation des premiers soins ou des traitements médicaux (physiques et psychologiques) pour la (les) personne(s) concernée(s). Lors de l'organisation d'un débriefing factuel à des fins de collecte d'informations, il est néanmoins important de garder à l'esprit les principes de base des premiers secours psychologiques : débriefing lorsque la sécurité physique et psychologique de base est assurée, création d'un espace sûr, responsabilisation de la victime, le processus, les attentes et les actions de suivi, etc[38].

Un débriefing factuel ne doit pas être confondu avec un débriefing émotionnel (également appelé désamorçage). Un événement traumatisant devrait être traité par des professionnels ou du personnel qualifié fournissant des PSP.

Les informations ci-dessous ne sont pas une tentative de former les lecteurs sur les Premiers Soins Psychologiques (PSP), ou de devenir des enquêteurs professionnels. Il s'agit d'une liste de conseils pour mener des entrevues sûres et utiles aux fins d'établissement des faits, dans le cadre de la déclaration des incidents.

Au début d'un débriefing factuel, rappelez à tous les participants que le but du débriefing est d'apprendre et de prévenir, et non de trouver la faute.

Préparation à un débriefing :

- Identifiez qui effectue le débriefing.
- Identifier qui est présent ; les procédures organisationnelles doivent définir si le personnel impliqué dans l'incident doit être présent ensemble ou séparément. La procédure peut indiquer que c'est un choix qui doit être fait au cas par cas, en fonction de la nature de l'événement et des contraintes logistiques. Bien que l'organisation d'un débriefing collectif présente clairement des avantages (logistiques, mais aussi pour la saisie du récit), elle peut aussi entraîner une réécriture de l'incident et une modification des faits (les témoins et les victimes s'influencent, leurs perceptions varient, le personnel peut craindre de donner des opinions sur les causes et les responsabilités devant les autres, etc.).

[38] Pour plus d'informations sur le PFA, voir les directives de l'Organisation mondiale de la santé cliquez ici.

- Informez les personnes faisant l'objet d'un débriefing de qui sera présent pendant celui-ci.
- Identifiez un espace sûr pour que le débriefing ait lieu. Choisissez un endroit sûr et pratique pour la personne, comme une salle de conférence ou un bureau privé.
- Permettre à la personne chargé du débriefing de suggérer le meilleur moment (en tenant compte des autres contraintes), en accord avec les procédures de débriefing de votre organisation.
- Préparez vos questions ; les questions peuvent suivre le modèle de rapport d'incident et couvrir les mêmes éléments. Vous pourriez ne pas avoir besoin de leur demander pendant l'entrevue mais ils vous guideront si nécessaire. Elles doivent être des questions ouvertes.
- Pratiquez la conscience de soi en identifiant vos propres biais potentiels et en les mettant de côté pendant le débriefing. L'analyse viendra plus tard.

Étapes du débriefing :

1. Conduisez l'interview dans un endroit calme et privé. Mettez l'individu à l'aise quand il arrive et offrez un verre d'eau, du thé ou du café. Assurez-vous qu'ils ne sont pas fatigués et qu'ils ont été débriefés émotionnellement.
2. Indiquer que le but du débriefing est l'établissement des faits et non la recherche des fautes.
3. Ne promettez pas la confidentialité, mais dites à la personne que vous partagerez l'information avec seulement ceux qui ont besoin de savoir.
4. Fournissez à la personne une estimation approximative du temps que prendra le débriefing.
5. Demandez à l'individu de raconter sa version de ce qui s'est passé sans l'interrompre. Prenez des notes ou enregistrez leurs réponses.
6. Posez des questions de clarification pour remplir les informations manquantes. Utilisez des questions ouvertes.
7. Raconter l'information obtenue à la personne interrogée. Corrigez les incohérences.
8. Demandez à l'individu ce qui, selon lui, aurait pu prévenir l'incident, en se concentrant sur les conditions et les événements qui ont précédé l'événement. Cela peut compléter l'analyse.
9. Évitez d'exprimer vos pensées, vos opinions ou vos conclusions au sujet de l'incident ou de ce que dit l'individu.
10. Informez la personne interrogée des prochaines étapes.
11. Remerciez l'individu.
12. Terminez la documentation du débriefing en remplissant le modèle de rapport d'incident.

Exemples de questions ouvertes :

- Où étiez-vous au moment de l'incident ?
- Que faisiez-vous à ce moment-là ?
- Qu'avez-vous observé qui aurait pu être inhabituel ?
- Qu'avez-vous vu ou entendu ?
- Quelles étaient les conditions environnementales (temps, lumière, bruit, etc.) à ce moment-là ?

- Que faisaient les travailleurs blessés à ce moment-là ?
- Selon vous, qu'est-ce qui a causé l'incident ?
- Comment, selon vous, des incidents similaires pourraient-ils être évités à l'avenir ?
- Y a-t-il d'autres témoins? Connaissez-vous les noms d'autres témoins ?
- Comment êtes-vous connecté avec les autres personnes impliquées dans l'incident ?
- Quels autres détails aimeriez-vous partager ?

Ce qu'il faut éviter :

- Intimider, interrompre ou juger l'individu.
- Aider l'individu à répondre aux questions.
- Poser des questions suggestives.
- Poser plusieurs questions en même temps.
- Devenir émotionnellement impliqué.
- Sauter aux conclusions.
- Révéler les découvertes de l'enquête.
- Faire des promesses qui ne peuvent être tenues.

Analyse :

Afin de responsabiliser l'individu et lui donner l'opportunité de partager des commentaires perspicaces, il est suggéré que vous lui demandiez son analyse de l'incident lors du débriefing. Néanmoins, rappelez-vous que leur jugement peut être affecté par l'événement traumatique. Les causes de l'incident devront être analysées par la personne qui remplit le rapport d'incident. Le but du débriefing d'établissement des faits est de déterminer tous les facteurs qui ont contribué à la survenue de l'incident.

Les questions suivantes peuvent vous aider dans votre analyse des facteurs :

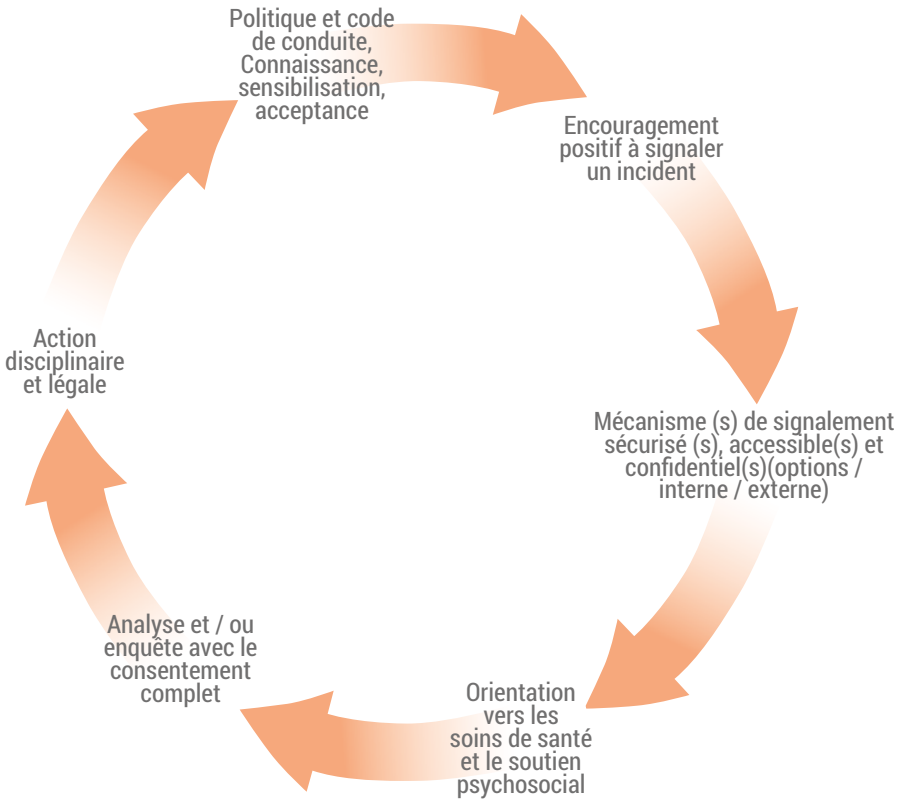
- Une situation dangereuse était-elle un facteur contributif ?
- L'emplacement était-il un facteur contributif ?
- La procédure a-t-elle été un facteur contributif ?
- Le manque d'équipement de protection individuelle ou d'équipement d'urgence a-t-il joué un rôle ?
- Les POS étaient-elles un facteur contributif, et devraient-elles être mises à jour pour refléter une nouvelle réalité sur le terrain?
- La dynamique de l'équipe a-t-elle été un facteur contributif et comment pensez-vous que nous pourrions l'améliorer ?

Des déclarations telles que « le personnel était négligent » ou « l'employé n'a pas suivi les procédures de sécurité », « mauvais moment, mauvais endroit » ne sont pas à la source d'un incident. Pour éviter ces conclusions trompeuses, concentrez-vous sur les raisons de l'incident, par ex. « Pourquoi l'employé n'a-t-il pas suivi les procédures de sécurité ? »

OUTIL 7 : BONNES PRATIQUES EN MATIÈRE DE SIGNALEMENT DES INCIDENTS LIES AU GENRE ET MÉCANISMES DE PLAINTES POUR SIGNALER L'EXPLOITATION ET LES ABUS SEXUELS (EAS)

Cet outil propose un résumé des bonnes pratiques en matière de signalement et de suivi des incidents liés au genre et les EAS. Il doit aider les organisations à développer et adapter leurs propres systèmes.

Cycle de signalement des incidents sensibles[39]



[39] Cet outil est extrait de Persaud, C. (2012). Genre et sécurité: Lignes directrices pour l'intégration du genre dans la gestion des risques de sécurité. EISF.

Politique :
La politique est à la base de la bonne déclaration des incidents et peut inclure une clause de dénonciation. Un accent particulier devrait être mis sur le suivi des rapports d'incidents. Il devrait y avoir des rapports obligatoires pour des incidents spécifiques, sauf dans les situations où il s'agit d'une option pour un individu, comme les cas de harcèlement et de violence liée au genre. L'exploitation et les abus sexuels relèvent d'un code de conduite et d'une politique différente. Les membres du personnel ont le devoir de signaler les cas d'exploitation et d'abus sexuels ou sinon de faire l'objet de possibles mesures disciplinaires (voir ci-dessous pour plus d'informations).

Conscience :
Le personnel doit être conscient de ce qui constitue un incident, en mettant particulièrement l'accent sur les situations moins discutées telles que le harcèlement, la violence liée au genre, les accidents évités de justesse ou les incidents mineurs. La sensibilisation peut être augmentée tout en créant du réconfort et de la confiance en encourageant les rapports d'incidents pendant l'induction, les orientations, les formations, les réunions, etc. Le personnel doit connaître ses droits et ses options.

Options / procédures de signalement d'incident :
Plusieurs canaux devraient être établis pour le signalement des incidents. Cela offre des options supplémentaires pour le personnel en fonction de leur niveau de confort ou de leur besoin de confidentialité. Les options comprennent (mais ne sont pas limitées à) : rapports en ligne via l'intranet, la hot line téléphonique (en PCV ou sans frais), points focaux, canaux qui contournent certains niveaux hiérarchiques (dans les cas où ils sont signalés) etc.

Utilisation des points focaux :
Les points focaux doivent être soigneusement sélectionnés et formés en fonction de leur profil personnel, de leurs capacités, de leur habilité à maintenir la confidentialité et de leur objectivité. Avoir un nombre varié de points focaux aux profils divers (internationaux et nationaux, hommes et femmes) peut augmenter l'aisance et l'accès aux procédures de signalement.

Analyse / enquêtes :
Le suivi des incidents éclairera par la suite l'analyse des risques, les mesures de réduction des risques ou les niveaux de sensibilisation du personnel. Un certain niveau d'enquête interne, mené par des personnes extrêmement bien formées, peut être nécessaire en cas de violation des politiques internes. Cela justifiera de notifier les autorités locales / police pour enquête externe en cas de violation confirmée des lois locales.

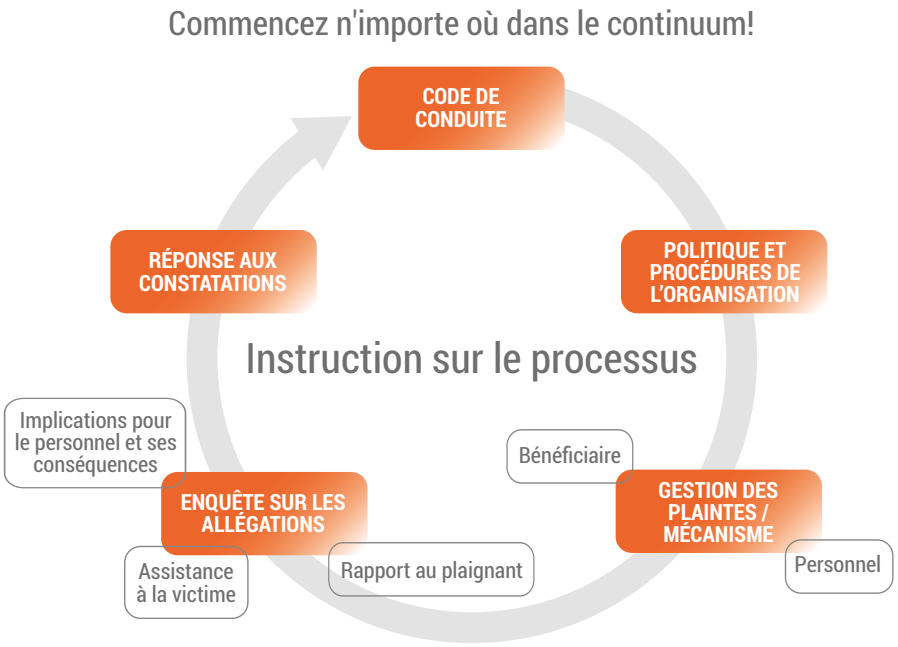
Procédures disciplinaires :
En cas de faute de la part d'un membre du personnel (en fonction de la gravité de l'incident et des lois locales, notamment du droit du travail), des mesures disciplinaires doivent être prises et appliquées de la même façon au personnel qu'il soit local / national / international / masculin ou féminin.

Mémoire institutionnelle :
Évitez d'engager toute personne ayant des antécédents de perpétration de tout type d'incident grave, y compris la corruption, le harcèlement sexuel ou la violence sexuelle, y compris l'exploitation sexuelle, les abus sexuels et la violence domestique. Cela peut sembler évident, mais il y a une longue histoire, à travers des exemples anecdotiques, d'auteurs réembauchés dans un pays différent parfois même par la même organisation. Si les lois pertinentes régissant les employeurs et les employés le permettent, coordonner avec d'autres organismes pour établir un système d'échange de renseignements sur les employés dont les contrats ont été résiliés pour harcèlement, violence sexuelle ou EAS. Des pratiques d'embauche prudentes qui comprennent la vérification des références et un contrôle sont impératives.

Cadre d'exploitation et d'abus sexuels (EAS) :
Principes d'EAS définis par l'Inter Agency Standing Committee (IASC)

- L'exploitation et les abus sexuels commis par des travailleurs humanitaires constituent des fautes graves et sont donc des motifs de licenciement ;
- Les relations sexuelles avec des enfants (personnes de moins de 18 ans) sont interdites quel que soit l'âge de la majorité ou l'âge du consentement localement. La croyance erronée dans l'âge d'un enfant n'est pas une défense ;
- L'échange d'argent, d'emploi, de biens ou de services à des fins sexuelles, y compris les faveurs sexuelles ou d'autres formes de comportement humiliant, dégradant ou d'exploitation, est interdit. Cela comprend l'échange d'assistance due aux bénéficiaires ;
- Les relations sexuelles entre les travailleurs humanitaires et les bénéficiaires sont fortement découragées car elles sont basées sur des dynamiques de pouvoir intrinsèquement inégales. De telles relations compromettent la crédibilité et l'intégrité du travail d'aide humanitaire ;
- Lorsqu'un travailleur humanitaire a des préoccupations ou des soupçons concernant des abus sexuels ou d'exploitation par un collègue, que ce soit dans la même organisation ou non, il / elle doit signaler ces préoccupations par le biais des mécanismes de signalement établis des organisations ;
- Les travailleurs humanitaires sont tenus de créer et de maintenir un environnement qui prévient l'exploitation et les abus sexuels et promeut la mise en œuvre de leur code de conduite. Les responsables à tous les niveaux hiérarchiques ont des responsabilités particulières pour soutenir et développer des systèmes qui maintiennent cet environnement.

Cycle de rapport EAS[40]



Source : Guide InterAction et ses modules d'apprentissage sur la lutte contre l'EAS.

40 InterAction. (2010). *Guide étape par étape d'InterAction sur la lutte contre l'exploitation et les abus sexuels.* InterAction.

OUTIL 8 : PLAN D'ACTION POUR LE SUIVI DES INCIDENTS

Cet outil répertorie les questions à inclure dans le plan d'action, qui devrait être mis en œuvre après chaque incident, quel que soit sa gravité.

Numéro de référence de l'incident : #

Action à prendre (une ligne par action)	Description de l'action à prendre en termes précis
Par qui	À quel niveau, nom ou position ?
Par qui	Qui va être impliqué, en interne ou externe à l'organisation ?
Logistique requise et budget	Coûts et besoins estimés, procédures d'achats l'organisation
Quand ?	Quand est-ce que l'action doit être mise en œuvre? Date fixe ou revue périodique ?
Qui est responsable de l'action mise en œuvre	Le responsable hiérarchique est-il responsable de cela ? Le SFP ? Quelqu'un d'autre ?
Revue et validation	Par qui et quelle date ?
Signature	Signature du personnel impliqué dans la mise en œuvre et dans le contrôle

Statut de l'incident :
Statut de gestion de l'incident :

OUTIL 9 : SYSTÈMES GIIS

Systèmes accessibles pour signaler, enregistrer, stocker et analyser les incidents de sécurité affectant l'organisation au niveau central.

ENREGISTREMENT D'INCIDENT ET MÉTHODE DE RAPPORT	SYSTÈME	AVANTAGES	DÉSAVANTAGES	ÉLÉMENTS DE COÛT DE MISE EN ŒUVRE ET DE FONCTIONNEMENT
Récit écrit de l'incident	• Courriels • Feuille Google • Plate-forme Google partagée • SharePoint	Coût d'installation très faible	Ne fonctionne bien que s'il est utilisé systématiquement. Risques : • Savoir-faire et parfois même accès perdu à l'occasion du départ du personnel. • Rapports très inégaux ; avec des implications pour la comparabilité de l'information. Nécessite beaucoup de temps au cours du processus d'analyse. process.	Coût lié au temps passé par le personnel pour la mise en place du système. Coût lié au temps passé par le personnel pour rédiger les rapports narratifs. Coût lié au temps passé par le personnel pour transformer l'information en un format systématique. Coût lié au temps de travail du personnel pour effectuer l'analyse. Cette partie peut prendre beaucoup de temps car le système lui-même ne prend pas en charge l'analyse.

ENREGISTREMENT D'INCIDENT ET MÉTHODE DE RAPPORT	SYSTÈME	AVANTAGES	DÉSAVANTAGES	ÉLÉMENTS DE COÛT DE MISE EN ŒUVRE ET DE FONCTIONNEMENT
Feuille de calcul Excel pour enregistrer les incidents à l'aide d'un codage systématique	Feuille de calcul Excel configurée pour les champs à enregistrer. La feuille de calcul Excel peut être utilisée pour classer systématiquement les informations soumises dans un format écrit.	Faibles coûts d'installation. Aucun coût de consultant requis car le travail peut facilement être fait en interne. Peut très bien fonctionner pour les organisations qui commencent à enregistrer des incidents et qui ont un nombre limité d'incidents à enregistrer et à gérer.	Peut devenir difficile à gérer lorsque trop de catégories et de types d'événements sont suivis. Nécessite une analyse de tendance très manuelle qui peut prendre beaucoup de temps. Seule la personne ayant accès à la feuille de calcul a tendance à connaître et à comprendre le système. Moins d'incitation pour le personnel à signaler car ils peuvent ne pas être conscients du système d'enregistrement.	Coût lié au temps passé pour développer un système Excel approprié. Le cout du personnel traduisant l'information écrite en catégories codées. Le coût du personnel pour effectuer l'analyse.
Abonnement à une plateforme en ligne pour la gestion des données	Certaines entreprises privées et certains organismes à but non lucratif offrent des plateformes en ligne pour la gestion de l'information issue des incidents de sécurité.	Systèmes efficaces dans les fonctions d'analyse intégrées. La plupart des systèmes permettent différents niveaux d'accès permettant un accès sur mesure pour le personnel de terrain ainsi que pour la direction. Les problèmes techniques sont externalisés. L'accès direct pour le personnel de terrain augmente l'incitation à signaler. Assure une fourniture de l'information plus élevée et systématique puisque tout le monde utilise le même système avec les mêmes instructions. Réduit la charge de travail du personnel d'analyse du Siège, car l'analyse peut être une fonction intégrée.	Coûts de fonctionnement mensuels Il peut être difficile ou coûteux de demander des modifications pour adapter le système aux exigences spécifiques à l'organisation	Frais d'inscription

ENREGISTREMENT D'INCIDENT ET MÉTHODE DE RAPPORT	SYSTÈME	AVANTAGES	DÉSAVANTAGES	ÉLÉMENTS DE COÛT DE MISE EN ŒUVRE ET DE FONCTIONNEMENT
Système en ligne personnalisé	Certaines organisations ont commandé le développement de systèmes en ligne spécifiques à l'organisation. Certaines organisations ont pu utiliser les systèmes existants et créer des rapports en tant qu'extension des plates-formes existantes utilisées pour le courrier électronique, telles que SharePoint.	Le système correspond aux besoins organisationnels et aux définitions internes. S'il est connecté à des systèmes existants, le personnel peut apprendre à l'utiliser beaucoup plus rapidement.	Coûts de développement élevés si des spécialistes informatiques externes sont nécessaires. Si les organisations peuvent utiliser leur département informatique, les coûts sont moins élevés. Les coûts de maintenance peuvent être élevés si il est nécessaire d'utiliser des consultants informatiques externes, mais moins si elle est assurée par le service informatique interne.	Coûts de développement et de maintenance

OUTIL 10 : CONSERVATION DE L'INFORMATION ISSUE DES INCIDENTS

Structures de base à utiliser sur les feuilles Excel pour enregistrer les incidents
Concevoir la structure idéale pour stocker de l'information issue des incidents de sécurité sur une feuille de calcul Excel est une tâche très difficile. Le large éventail d'événements différents qui devraient être pris en compte pour la prise de décision stratégique dans le contexte de la sécurité et les informations détaillées requises sur certains aspects rendent impossible l'existence d'une structure simple adaptée à toutes les situations. Le défi consiste à trouver le juste équilibre entre le maintien de la simplicité et de la praticabilité tout en conservant les informations clés requises, avec suffisamment de détails pour que l'information soit significative pour émettre des recommandations.

Ce guide fournit deux exemples de format différents sur la façon dont l'information issue des incidents peut être stockée dans une feuille de calcul Excel. Les organisations qui conçoivent leur propre feuille de calcul sont encouragées à regarder les exemples fournis et à mélanger et assortir les éléments les plus adaptés à leurs propres priorités. Veuillez consulter d'autres outils pour les définitions suggérées des différents domaines.

Les deux exemples de feuilles de calcul Excel pour l'enregistrement des incidents peuvent être consultés et téléchargés à partir de la page du projet RedR. Voir les éléments ci-dessous :

- Feuille de calcul des catégories d'événements SiND
- Modèle de journal d'incident

Vous trouverez ci-dessous les principes clés à prendre en compte lors de la conception d'une feuille de calcul Excel pour les informations sur les incidents de sécurité.

Unités d'analyse
Chaque ligne d'une feuille de calcul Excel stocke une unité clé d'information. Dans la plupart des cas, ce sera l'événement. Chaque ligne est un événement unique. Les colonnes sont utilisées pour fournir des détails sur l'événement.

Pour enregistrer d'autres unités d'information, comme traiter les membres du personnel comme des unités individuelles (plutôt qu'un numéro associé à un événement), ou enregistrer des détails sur le matériel perdu ou suivre une réponse, on peut procéder de la manière suivante :

- Créez une deuxième / troisième / quatrième feuille sur le classeur Excel pour 'personnel', 'matériel' ou 'réponse'. Sur ces nouvelles feuilles de calcul, chaque rangée stocke les informations individuelles sur chaque personne, chaque élément endommagé ou perdu, ou chaque réponse, etc. Chaque feuille de calcul compte donc une unité différente. Si quatre membres du personnel sont affectés en une seule fois, la feuille de calcul de l'événement comporte une rangée (une unité) pour l'événement mais quatre rangées (quatre unités) pour le personnel (voir les exemples ci-dessous). Si deux voitures sont endommagées, la «feuille de matériel» comporte deux rangées, une pour chaque voiture. Chaque membre du personnel et chaque voiture deviennent ainsi une unité à part entière. Ces feuilles peuvent être utilisées pour stocker des détails utiles à l'analyse globale.

  - L'avantage d'un tel système est qu'il devient plus facile de fournir une analyse détaillée au-delà de la description de l'événement. Il est également possible d'utiliser des listes déroulantes de plusieurs catégories exclusives choisies pour chaque individu. La feuille contient plus d'informations sous une forme plus condensée. L'inconvénient est que les données deviennent plus complexes.
  - Si des feuilles de calcul supplémentaires sont ouvertes, il est essentiel d'utiliser des numéros d'identité d'événement uniques dans la première colonne pour s'assurer qu'il est possible de relier les informations à l'événement.

- Intégrez une unité différente (telle que le personnel, le matériel) dans la feuille où l'unité d'analyse est l'événement. Cela peut être fait en créant une série de colonnes supplémentaires chaque fois que l'unité de comptage est changée d'événement en personnel, matériel ou réponse. Différentes couleurs peuvent être utilisées pour l'indiquer.

  - Par exemple, les colonnes pourraient inclure le nombre de personnes affectées par l'événement par autant de colonnes supplémentaires que nécessaire pour classer tout le personnel par des informations supplémentaires, qui doivent ensuite être divisées en plusieurs colonnes d'options (voir la base de données Aid Worker Security Database comme un exemple de comment les informations détaillées sur le personnel peuvent être enregistrées les unes à côté des autres).

Quelques différences d'informations sur les feuilles Excel simples ou multiples
Les exemples ci-dessous montrent les mêmes informations sur quatre personnes affectées dans un même événement, stockées par unité d'analyse « événement » et unité d'analyse « personnel ». Stocker les informations sur le personnel sur une feuille de calcul où l'unité d'analyse est l'événement nécessite plus de colonnes pour stocker moins de détails. Il n'est pas non plus possible de stocker des détails sur les individus (il serait très difficile d'ajouter les informations supplémentaires sur le travail ou si l'assurance prenait en charge le soutien psychologique post incident). Si le personnel constitue l'unité d'analyse, il est facile d'enregistrer des informations plus détaillées. Ce détail supplémentaire pourrait aider à repérer les tendances ou à identifier des recommandations d'action spécifiques, par exemple en matière de prise en charge par l'assurance.

Feuille unique pour les unités d'événement :

UNITÉ D'ANALYSE	NOMBRE DE MEMBRES DU PERSONNEL AFFECTÉS	FEMME	HOMME	MEMBRE DU PERSONNEL INTERNATIONAL	MEMBRE DU PERSONNEL NATIONAL	AUTRE	MORTS	BLESSÉS
Event 1	4	1	3	1	2	1	1	3

Plusieurs feuilles pour différentes unités (par exemple personnel, matériel ou réponse) :

UNITÉ D'ANALYSE	IDENTITÉ D'ÉVÉNEMENT UNIQUE	SEXE	STATUT	EMPLOI	IMPACT	PRISE EN CHARGE PAR L'ASSURANCE DU SOUTIEN PSYCHOLOGIQUE
Personnel 1	Évènement 1	Femme	Membre du personnel international	Personnel professionnel	Blessé	Couvert
Personnel 2	Évènement 1	Homme	Membre du personnel national	Chauffeur	Mort	Non applicable
Personnel 3	Évènement 1	Homme	Membre du personnel national	Personnel professionnel	Blessé	Pas couvert
Personnel 4	Évènement 1	Homme	Volontaires	Volunteer	Blessé	Pas couvert

Options multiples ou mutuellement exclusives
Les informations peuvent être enregistrées en tant qu'options multiples (plus d'une description s'applique) ou en tant qu'options mutuellement exclusives (une seule option peut s'appliquer).

- **Plusieurs options** sont présentées dans des colonnes l'une à côté de l'autre. Chaque colonne représente une caractéristique particulière et la feuille de calcul est utilisée pour indiquer que l'option spécifique s'applique à l'événement. Cela peut être fait en choisissant « oui », un nombre (par exemple « 1 ») ou une option dans une liste déroulante. Les options qui ne s'appliquent pas sont soit laissées vides (moins de travail dans le codage) soit identifiées comme ne s'appliquant pas en choisissant « non applicable » ou « 0 » (cela permet de vérifier que les nombres totaux sont corrects et de repérer les erreurs).
- **Les options mutuellement exclusives** sont présentées sous la forme d'options de liste déroulante qui peuvent être choisies lors du remplissage d'informations dans une colonne particulière. Les listes déroulantes vous permettent d'enregistrer des informations supplémentaires et d'assurer la cohérence de l'orthographe. Cependant, elles ne devraient être utilisées que si une seule option peut s'appliquer. Voir la feuille de calcul des catégories d'événements SiND pour des exemples de menus déroulants.
- **Des options multiples et mutuellement exclusives** peuvent être combinées dans la gestion des données. Une feuille de calcul bien conçue peut contenir une série de colonnes présentant plusieurs options (par exemple, toutes ou certaines des options peuvent s'appliquer à chaque événement et les colonnes sont remplies si nécessaire). Ces options ont une liste associée d'options de listes déroulantes mutuellement exclusives (par exemple, chaque fois qu'une des options est choisie, le système indique non seulement « oui » ou un nombre mais spécifie la sous-catégorie sous l'option). Pour un exemple d'un tel système, voir la feuille de calcul des catégories d'événements SiND.

OUTIL 11 : TECHNOLOGIE POUR SIGNALER ET ENREGISTRER LES INCIDENTS

Chaque système pour signaler et enregistrer les incidents est différent et a ses propres avantages et inconvénients. Le modèle le plus approprié à une organisation dépendra de son niveau de capacité technologique, de l'échelle de ses opérations, de sa taille et de ses ressources financières, etc.

Voir le tableau ci-dessous pour une comparaison de certains systèmes de rapports d'incidents en ligne[41].

	GRATUIT	SOURCE OUVERTE (GRATUIT)	AUTORISÉ	AUTONOME	LOGICIEL EN TANT QUE SERVICE	STANDARD	FAIT SUR MESURE	GRAPHIQUES INTÉGRÉS	NIVEAU DE PROTECTION DES DONNÉES
Ushahidi		●		●		●			●●
SIMSON	●		●		●	●		●	●●
Open DataKit		●		●		●		●	●●
SharePoint	●		●	●	●	●		●	●●
NAVEX Global™	●		●		●		●	●●	●●
IRIS	●		●				●	●	●●
RIMS			●				●	●	●●

●● Non analysé

La section suivante présente les avantages et les inconvénients des systèmes actuellement utilisés par les organisations qui ont contribué à ce manuel. Pour en savoir plus sur un système, veuillez suivre les liens fournis.

41 Certaines des informations partagées dans cet outil ont été extraites d'un article non publié de l'EISF: De Palacios, G. (2017). « Gérer les informations liées à la sécurité: un examen plus approfondi des systèmes de signalement des incidents », *EISF*.

SharePoint

Ceci est une application Web qui s'intègre à Microsoft Office. Il est principalement vendu comme système de gestion et de stockage de documents. Cependant, le produit est hautement configurable et l'utilisation varie considérablement entre les organisations. Bien qu'il nécessite l'achat d'une licence pour son utilisation, certains des produits Microsoft Office 365 sont gratuits pour les organisations à but non lucratif. SharePoint est un système qui peut être utilisé pour partager des informations sous différentes formes; il est possible de créer des formulaires en ligne auxquels seuls les utilisateurs autorisés peuvent accéder.

AVANTAGES	LIMITES
En tant que produit Microsoft, il est compatible avec les logiciels de traitement de données tels que Word, Excel, PowerPoint, etc. Cela permet à une organisation d'exporter facilement les données du système vers ces applications et de partager et analyser les informations à l'aide d'un logiciel familier. Elles pourraient ne pas avoir besoin d'une nouvelle installation de logiciel ou de formation du personnel sur l'utilisation de la nouvelle plate-forme. Le développement du système peut être géré en interne par l'équipe informatique déjà en charge du développement et de la maintenance de SharePoint.	Bien qu'il soit possible d'exécuter des enquêtes à l'aide de SharePoint, il ne s'agit pas d'un logiciel spécialement conçu pour signaler ou collecter des données. La représentation des données dans une carte n'est pas intégrée par défaut dans le système et il faudrait le faire en installant un module supplémentaire.

Ushahidi

Ushahidi a été développé pour cartographier la violence au Kenya pendant et après les violences post-électorales en 2008. Les rapports peuvent être envoyés via un certain nombre de plateformes, y compris un formulaire en ligne, un e-mail, un message texte ou des réseaux sociaux tels que Twitter. Une fois ces rapports reçus, ils peuvent être revus par un administrateur afin de valider et d'approuver le contenu, afin qu'ils puissent apparaître sur la carte de sa page principale.

Ushahidi est un logiciel libre et gratuit pour la collecte d'informations, la visualisation et la cartographie interactive. Le formulaire de rapport peut être personnalisé afin qu'une organisation puisse collecter les informations qui sont importantes pour elle, et une fois les rapports validés, il est possible de les voir reflétés dans une carte regroupée selon la catégorie d'incident prédéfinie. La plate-forme peut être programmée pour alerter les responsables de la sécurité lorsqu'un nouvel incident a été signalé, afin qu'ils puissent apporter un soutien aux victimes et valider le rapport. Ushahidi peut également alerter les autres utilisateurs une fois le rapport validé.

AVANTAGES	LIMITES
Le principal avantage d'Ushahidi est qu'il peut être téléchargé gratuitement sur Internet. L'installation du système n'est pas compliquée et puisque l'organisation décide où installer le logiciel, les données restent sous le contrôle de l'organisation.	Le principal inconvénient d'Ushahidi est que la représentation statistique des informations contenues dans la base de données n'est pas intégrée dans le système, et que des solutions externes doivent être combinées à cette fin. C'est une excellente solution pour la collecte de données, mais d'autres ressources sont nécessaires pour l'analyse des données. La plate-forme Ushahidi n'est plus en cours de développement, ce qui pourrait causer des problèmes au fur et à mesure que d'autres technologies connexes évoluent. Ces problèmes potentiels peuvent éventuellement être résolus par le personnel informatique.

SIMSON

Le système SIMSON a été spécialement conçu pour les ONG par le Center for Safety and Development (CSD). SIMSON est un système de signalement des incidents de sécurité en ligne où les utilisateurs peuvent voir les incidents signalés représentés sur une carte. Les ONG qui utilisent SIMSON ne doivent pas installer, programmer ou écrire le code d'un logiciel. Le Center for Safety and Development (CSD) fournit également un support pour l'exécution de la plateforme et la gestion des sauvegardes. Les incidents peuvent être filtrés par catégories, organisation, lieu, calendrier et autres informations et indicateurs liés à la sécurité. Les utilisateurs reçoivent des alertes par e-mail des nouveaux rapports d'incidents en fonction de leur place dans l'organisation et de leurs droits d'accès dérivés. Les incidents peuvent être analysés dans SIMSON à l'aide de graphiques et de tableaux. Les données d'incident peuvent également être téléchargées sous forme de fichier Excel. Les documents et les rapports d'incidents peuvent être téléchargés et, à la discrétion de l'organisation, partagés avec d'autres parties prenantes, par exemple, des compagnies d'assurance ou d'autres ONG. Il existe une procédure spéciale « incident sensible » qui n'informe que les agents désignés de votre organisation. Ceci est pertinent lorsqu'il s'agit par exemple d'incidents d'agression sexuelle.

Pour en savoir plus, un aperçu de SIMSON peut être téléchargé à partir de la page Web du CSD en suivant ce lien.

AVANTAGES	LIMITES
Le système est prêt à l'emploi, à destination des ONG et soutenu par le CSD. Les organisations n'ont donc pas besoin d'investir des ressources dans son développement, sa maintenance, ses sauvegardes. Les données d'incident peuvent être analysées dans SIMSON ou en exportant les données dans un fichier Excel.	Bien que le CSD garantisse aux organisations utilisant le système que, si elles le souhaitent, elles sont les seules à pouvoir consulter leurs rapports d'incident, les ONG peuvent souhaiter contrôler leurs données relatives à la sécurité et aux incidents et hésiter à déléguer cette responsabilité à des tiers. La personnalisation du formulaire de rapport pour les besoins spécifiques de l'organisation peut ne pas être facile.

World Vision International and NAVEX Global

World Vision International (WVI), en partenariat avec le fournisseur international de rapports sur les risques NAVEX Global, a créé un système de signalement des incidents en ligne pour la communication d'incidents, de plaintes, de harcèlement et d'autres événements. Ce système va au-delà de la stricte communication des incidents de sûreté et de sécurité et englobe d'autres éléments d'une approche de gestion des risques tels que la corruption, les poursuites judiciaires, la réputation, etc., en plusieurs langues. NAVEX Global adapte son système de débriefing aux besoins et aux caractéristiques de l'organisation qui l'utilise. Le système de signalement des incidents permet la contribution de diverses sources et tout le personnel de WVI est en mesure de faire rapport sur la plate-forme, car il sert également de système de lanceurs d'alerte.

Pour en savoir plus sur le système de signalement des incidents World Vision International, consultez le document suivant.

AVANTAGES	LIMITES
La combinaison du formulaire de signalement d'incident avec le canal de lanceur d'alerte, le mécanisme de plainte des bénéficiaires, etc. réduit la diversité possible des systèmes utilisés à des fins similaires. Avoir le soutien d'une entreprise dédiée à la gestion de l'éthique et de la conformité derrière le système peut aider à mettre en perspective les données des rapports d'incidents avec d'autres domaines de gestion des risques.	Le formulaire peut être relativement détaillé, ce qui, malgré ses avantages, peut décourager les rapports en raison de son long processus. C'est probablement aussi une solution que seules les grandes organisations peuvent se permettre.

IRIS

Basé sur Ushahidi, IRIS est une plateforme qui peut être utilisée pour signaler des incidents via une interface en ligne, et visualiser où ces incidents ont eu lieu sur une carte. Il est possible de personnaliser le modèle de rapport d'incident pour répondre aux besoins de débriefing de l'organisation utilisant le système.

La plate-forme peut être utilisée en tant que « logiciel en tant que service », ainsi qu'en l'installant sur les serveurs d'une organisation, ce qui permet un contrôle total des données rapportées. Seuls les utilisateurs enregistrés peuvent accéder à l'interface et différents privilèges peuvent être définis en fonction du profil de l'utilisateur. Les rapports peuvent être soumis via l'interface en ligne ou via une connexion à faible bande passante.

La plate-forme est multilingue et les rapports peuvent être filtrés par défaut ou par des champs personnalisés. Les responsables et les autres utilisateurs peuvent être avertis lorsque de nouveaux incidents ont été signalés afin qu'un soutien immédiat puisse être fourni aux victimes pendant que le reste de l'équipe est informé pour prendre les mesures appropriées.

Les données peuvent être extraites de la plate-forme et transmises au logiciel de visualisation de données afin que les statistiques sur les incidents puissent être utilisées pour tirer les leçons apprises, donner des recommandations, fournir des briefings, utiliser comme information de base pour l'analyse des risques, etc.

AVANTAGES	LIMITES
Facile à installer et à utiliser, hautement personnalisable dans son apparence et dans la façon dont les informations sont collectées. IRIS est basé sur Ushahidi version 2, qui est une plate-forme open source, peut être développé pour répondre aux besoins de débriefing des organisations qui l'utilisent, pour l'adapter aux nouveaux développements et technologies et pour le rendre compatible avec d'autres systèmes existants. Les utilisateurs sont illimités et fonctionnent sans licence. Les organisations ne paient donc que pour l'installation et la personnalisation. Les données existantes sur les incidents peuvent être importées dans le système lors de l'installation.	La connexion de la liste des utilisateurs avec le répertoire actif de l'organisation devrait être développée, mais les utilisateurs peuvent être créés un par un et accéder aux informations accordées au cours du processus. Le logiciel original a été conçu pour partager largement les informations rapportées. Bien qu'il soit possible d'avoir un profil utilisateur 'reporter uniquement', la limitation de l'accès à l'information doit être soigneusement planifiée.

RIMS

Le service de gestion des incidents de la Risk Management Society (RIMS) offre un système simple et facile à utiliser qui utilise principalement des descriptions d'incidents basées sur des tests. Il permet aux catégories personnalisées de coder les aspects des événements. Il est possible de créer des graphiques. La plate-forme existe uniquement en anglais.

Dans l'exemple considéré, le système était principalement utilisé par le département RH autour des assurances. L'utilisation du système pour l'analyse des incidents de sécurité était limitée. Il n'a donc pas été possible de déterminer si ce système aurait pu fonctionner correctement s'il avait été entièrement configuré pour répondre aux besoins de gestion de l'information issue des incidents de sécurité, au-delà des descriptions d'incidents basées sur les tests et en particulier des analyses.

AVANTAGES	LIMITES
Facile à utiliser. Le personnel peut utiliser le système pour signaler des incidents sans beaucoup de formation. Il est facile de configurer des champs personnalisés et de naviguer sur le site. C'est un système facile et très accessible pour stocker les descriptions d'incidents de sécurité.	L'exemple examiné utilisait principalement des descriptions d'événements basées sur du texte. Le système n'envoie pas de rappels.

OUTIL 12 : ANALYSE ET COMPARAISON DES TENDANCES DES DONNEES

Conseils lors de la comparaison des données de tendances d'organisation avec des données d'incident de sécurité plus larges.

Questions clés et considérations

- Quelles sont les similitudes et les différences dans les tendances entre votre organisation et celles qui apparaissent dans les données regroupées ?
- Pourquoi y a-t-il des similitudes et des différences ? Réfléchissez à chaque aspect observé séparément et demandez :
  - Pourquoi vois-je des similitudes ou des différences dans cette sous--catégorie de types d'incidents ?
  - Est-ce dû à l'environnement externe général ?
  - Comment ces tendances sont-elles affectées par les pays dans lesquels votre organisation travaille ou les programmes mis en œuvre par votre organisation ?
  - Est-ce que l'une ou l'autre des différences pourrait être le résultat de pratiques de signalement (les vôtres ou celles d'autres organisations) ?
  - Où votre organisation a-t-elle plus d'incidents d'un type particulier ?
  - Où votre organisation a-t-elle moins d'incidents d'un type particulier ?
- Rechercher des similitudes dans les tendances et essayer de donner une explication des similitudes.
- Regardez les différences. Essayez de suggérer une explication pour les différences.
- Assurez-vous d'être précis. Si vous êtes sûr qu'un élément est un fait, dites-le. Si vous le pensez mais n'avez pas de preuve, utilisez des termes comme « les données suggèrent », ou «il apparaît à partir des informations disponibles ».
- Identifier les tendances clés :
  - Quelles tendances clés peuvent être repérées ?
  - Les données suggèrent-elles des tendances émergentes dont les organisations doivent tenir compte ?
- Décrivez les tendances aussi spécifiques que possible.
  - Ces tendances sont-elles mondiales ?
  - Y a-t-il des tendances dans un pays spécifique ?
  - À quelle catégorie d'événements de sécurité se réfèrent-ils ?
  - Soyez aussi précis que possible en nommant les types d'incidents que vous voyez augmenter et où cela peut se produire. Si vous le pouvez, fournissez des détails sur qui ou quoi peut être particulièrement affecté.

- Réfléchissez aux tendances générales du contexte global de l'aide telles qu'elles apparaissent dans l'analyse des tendances ou qu'elles soient visibles dans les données au niveau mondial ou national. Essayez de décrire le contexte général de la distribution de l'aide, les changements récents, les menaces ou tendances émergentes.
- Pensez aux différences de tendances entre les données de votre organisation et celles des autres organisations (à l'exclusion de celles qui résultent des différences de signalement). Tenez compte des pays dans lesquels votre organisation travaille, des programmes offerts par votre organisation et des faiblesses ou points forts du cadre de gestion des risques de sécurité de votre organisation.
- Si vous le faites une seconde ou une troisième fois, pensez aux différences entre les données les plus récentes et les analyses précédentes. Décrivez les changements et suggérez des explications.
- Identifier les mesures à prendre :
  - Y a-t-il des questions émergentes de l'examen des données que vous pourriez suivre ?
  - Qui peut vous aider à en savoir plus ?
- Contactez le pays / bureau régional / fournisseur de services d'information avec des questions afin d'obtenir un aperçu de la réalité derrière les tendances de données.
- Pensez à ce que vous mettrez en œuvre dans votre plan d'action au cours des prochaines semaines / mois.

Développer un plan d'action

- Les données suggèrent-elles que le point focal de sécurité devrait prendre des mesures spécifiques ?
- Les données suggèrent-elles que de nouveaux risques émergents ou des situations d'escalade devraient être ajoutés aux formulaires de consentement éclairé à discuter avec le personnel ?
- Les données suggèrent-elles qu'un type d'événement particulier devrait être mis en évidence lors de la formation pour un contexte spécifique ?
- Les données mettent-elles en évidence les risques spécifiques qui devraient être discutés plus en détail avec les PFS nationaux et régionaux pour voir si des changements de politique sont nécessaires ?
- Les données mettent-elles en évidence les problèmes qui doivent être portés à l'attention de la hiérarchie dans l'organisation ?
- Votre analyse des données suggère-t-elle que votre organisation a besoin d'améliorations dans la gestion de l'information issue des incidents de sécurité à un certain niveau au sein de l'organisation ?

Problèmes éventuels à signaler aux collègues, que ce soit sur le terrain ou au niveau de la direction ou du conseil d'administration

- Nommez des tendances spécifiques qui devraient être surveillées de près. Suggérez-leur de les mettre régulièrement à l'ordre du jour.
- Mettre en évidence un risque particulier et spécifique et suggérer une discussion interne sur le seuil de risque acceptable pour un type particulier d'événement dans un contexte particulier pour aider à formuler une politique claire.

- Suggérer des activités spécifiques pour améliorer la gestion de l'information issue des incidents de sécurité afin d'améliorer la capacité de l'organisation à repérer les tendances et à demander la mise en œuvre d'éléments spécifiques (voir la grille d'évaluation pour un élément spécifique pouvant être amélioré).

Communiquez vos conclusions finales et votre plan d'action

Rédigez un document concis et clair qui :

- Mentionne les sources et les méthodes utilisées.
- Indique que vous avez pris en compte les données et que vous avez confiance dans vos résultats (vous pouvez inclure le fait que vous avez ignoré d'approfondir un aspect spécifique parce que vous pensez que c'est le résultat d'un biais de compte rendu).
- Dressez une liste claire des tendances qui vous préoccupent. Choisissez un maximum de trois. Si c'est un exercice régulier, incluez les tendances clés de l'analyse passée.
- Répertoriez l'action que vous recommandez :
  - Pour vous-même en précisant ce que vous avez fait, vous êtes en train de le faire ou que vous allez faire.
  - Au cours des prochains mois pour répondre aux besoins identifiés :
  - Pour d'autres collègues (sur le terrain ou la hiérarchie). Gardez ceux pour les autres à une seule tâche en suggérant comment vous allez faciliter le processus et ce que vous aurez besoin d'eux comme leur apport, de soutien.

Comparez vos données avec les données regroupées par Insecurity Insight via la base de données SiND d'Aid in Danger en utilisant l'analyse des tendances publiée ou en vous rendant à Humanitarian Data Exchange, en plus de vos données d'incidents de sécurité passés.

Voir un exemple de rapport d'analyse de données de tendance multi-organisations ici.

OUTIL 13 : QUESTIONS DE NIVEAU STRATÉGIQUE POUR LES DÉCISIONS RELATIVES À LA GESTION DE L'INFORMATION ISSUE DES INCIDENTS

Après une bonne vue d'ensemble du type d'incident de sécurité survenu, examinez les données et déterminez si elles indiquent une action de suivi requise. Recherchez des informations supplémentaires et mettez fin au rapport d'incident de sécurité avec des recommandations spécifiques.

La liste de questions suivante peut aider les points focaux de sécurité à élaborer des conclusions stratégiques et des recommandations d'action supplémentaires à la suite d'une bonne analyse des événements de sécurité.

QUESTIONS À PRENDRE EN COMPTE LORS DE L'ANALYSE DES DONNÉES D'INCIDENT DE SÉCURITÉ ANALYSÉES	ACTION DE SUIVI POSSIBLE	POSSIBLE RECOMMANDATION D'ACTION À RAJOUTER À LA FIN DU RAPPORT D'ANALYSE
1. Quels types d'incidents de sécurité le personnel et l'organisation ont-ils rencontrés? 2. Dans quels pays sont-ils apparus ?		
Notre organisation prépare-t-elle adéquatement le personnel au type d'événements possibles qu'il peut rencontrer ?	Identifiez dans quelle mesure les personnes ont été bien préparées pour les types d'événements qui se produisent. Identifiez le coût des formations pertinentes et ajoutez une estimation budgétaire.	Suggérer le besoin de formations spécifiques ou de sensibilisation pour le personnel travaillant dans des contextes affectés par des types d'incidents particuliers.
L'assurance couvre-t-elle les réponses requises pour le personnel ou pour faire face aux dommages matériels ?	Renseignez-vous auprès des employés concernés, qu'ils aient reçus ou qu'ils auraient aimé recevoir un soutien psychologique après un incident. Vérifiez si un tel soutien est couvert par l'assurance. Vérifiez à quel point il est facile ou au contraire coûteux de remplacer des objets perdus (assurance ou autre).	Suggérez des lacunes dans la couverture d'assurance. Proposer une stratégie pour faire face à la perte matérielle dans les contextes nationaux où cela semble être un risque accru.

QUESTIONS À PRENDRE EN COMPTE LORS DE L'ANALYSE DES DONNÉES D'INCIDENT DE SÉCURITÉ ANALYSÉES	ACTION DE SUIVI POSSIBLE	POSSIBLE RECOMMANDATION D'ACTION À RAJOUTER À LA FIN DU RAPPORT D'ANALYSE
3. En tant que point focal sécurité du siège, dans quelle mesure êtes-vous satisfait de la façon dont les bureaux de pays semblent avoir utilisé les incidents de sécurité et les incidents évités de justesse pour apprendre et améliorer leurs pratiques ? **4. Quels sont les incidents de sécurité rencontrés par d'autres organisations dans le même pays et comment cela se compare-t-il aux incidents signalés au sein de votre organisation ?**		
Y a-t-il des bureaux pays qui ne déclarent systématiquement pas leur incident au siège ?	Entamer un dialogue avec le personnel clé pour savoir pourquoi aucun ou seulement quelques incidents ont été signalés.	Recommander de revoir les instructions sur comment et quand signaler. Recommander de modifier le système de signalement de manière à encourager les rapports systématiques. Recommander un meilleur support de la part de la direction pour démontrer les avantages d'un débriefing systématique.
Y a-t-il des bureaux pays qui connaissent des types particuliers d'incidents ? Comment ces incidents se comparent-ils à ceux vécus par d'autres organisations ?	Entamer un dialogue avec le personnel clé pour savoir pourquoi des incidents particuliers se produisent fréquemment ou jamais.	
5. Comment les incidents de sécurité ont-ils affecté la fourniture de l'aide ? **6. Peut-on évaluer l'impact des incidents de sécurité sur la fourniture de l'aide ?**		
Vos collègues ont-ils signalé dans quelle mesure les incidents ont perturbé votre travail ?	Entamer un dialogue avec des collègues sur la meilleure façon de décrire l'impact des incidents de sécurité sur la livraison de l'aide.	Rajoutez des déclarations sur la manière dont les incidents de sécurité ont affecté la distribution de l'aide.
Vos collègues ont-ils chiffré la perte de temps et de perte matérielle du personnel ?	Entamer un dialogue avec le personnel sur la meilleure façon de faire perdre du temps au personnel et des biens matériels.	Rajoutez des déclarations sur coûts des incidents de sécurité pour les opérations.
Vos collègues ont-ils signalé dans quelle mesure l'incident de sécurité a affecté l'accès humanitaire?	Entamer un dialogue avec le personnel pour décrire comment la sécurité affecte l'accès aux populations bénéficiaires et combien de personnes pourraient ne pas être atteintes en raison de problèmes de sécurité.	Rajoutez des déclarations sur la façon dont les incidents de sécurité affectent l'accès aux populations bénéficiaires.

QUESTIONS À PRENDRE EN COMPTE LORS DE L'ANALYSE DES DONNÉES D'INCIDENT DE SÉCURITÉ ANALYSÉES	ACTION DE SUIVI POSSIBLE	POSSIBLE RECOMMANDATION D'ACTION À RAJOUTER À LA FIN DU RAPPORT D'ANALYSE
7. Quels étaient les principaux contextes d'incidents de sécurité ? **8. Le contexte des incidents peut-il être classé et quelle stratégie de réponse peut-être nécessaire ?**		
Combien d'incidents ont pu se produire en raison d'échecs dans une bonne stratégie d'acceptance ? Dans quels domaines y a-t-il eu un échec d'acceptance ? Acteurs non étatiques, autorités, bénéficiaires, personnel, entrepreneurs ou autres ?	Entamer un dialogue au sein de l'organisation sur la meilleure stratégie d'acceptance et comment la mettre en œuvre efficacement.	Nommer la zone ou la population cible pour laquelle une meilleure stratégie d'acceptance doit être développée. Suggérer une meilleure formation à la stratégie d'acceptance pour le personnel se rendant dans un pays spécifique pour traiter avec un acteur spécifique.
Combien d'incidents ont pu se produire parce que le personnel n'a pas respecté les règles ou les règlements ou s'est comporté de manière irresponsable ?	Entamer un dialogue au sein de l'organisation sur la meilleure façon de promouvoir le code de conduite éthique pour le personnel et assurer le respect des procédures de sécurité.	Énumérer les aspects de comportement qui pourraient être inclus dans un code de conduite personnel est tenu d'adhérer. Énumérer les domaines de comportement où le personnel ne respecte pas les règles et suggère un mécanisme pour mieux les appliquer.
Combien d'incidents ont pu se produire en raison de facteurs personnels liés à l'origine, aux antécédents ou aux liens familiaux du membre du personnel ?	Rechercher des conversations au sein de l'organisation sur la façon de traiter les facteurs de risque liés à la vie domestique, l'origine ethnique ou d'autres facteurs privés.	Dressez la liste des contextes et des pays où des politiques et procédures spécifiques peuvent être nécessaires, notamment : • Comment répondre si un membre du personnel est affecté par la violence domestique • Comment réagir lorsqu'il y a un risque de discrimination ethnique ou de violence • Quel code de conduite éthique à attendre du personnel local lorsque les intérêts commerciaux ou politiques de la famille élargie pourraient affecter le personnel.

QUESTIONS À PRENDRE EN COMPTE LORS DE L'ANALYSE DES DONNÉES D'INCIDENT DE SÉCURITÉ ANALYSÉES	ACTION DE SUIVI POSSIBLE	POSSIBLE RECOMMANDATION D'ACTION À RAJOUTER À LA FIN DU RAPPORT D'ANALYSE
7. Quels étaient les principaux contextes d'incidents de sécurité ? **8. Le contexte des incidents peut-il être classé et quelle stratégie de réponse peut-être nécessaire ?**		
Combien d'incidents sont survenus parce que le personnel ou l'organisation se trouvait au mauvais endroit au mauvais moment ?	Entamer un dialogue au sein de l'organisation dans quelle mesure est-elle prête à accepter les risques généraux liés au terrorisme, à la criminalité ou à d'autres incidents qui ne ciblent pas spécifiquement l'organisation.	Dresser la liste des pays présentant un risque accru d'incidents échappant au contrôle des meilleures politiques de sécurité.
Combien d'incidents sont survenus en raison de l'action des acteurs étatiques ?	Identifier les acteurs étatiques responsables dans les documents internes et essayer d'identifier des pistes pour rechercher un dialogue avec ces acteurs étatiques. Parlez à vos collègues de plaidoyer et envisagez de développer une campagne conjointe avec d'autres ONG pour sensibiliser le public.	Suggérer des voies possibles pour les conversations à suivre par les représentants des pays ou la direction en utilisant les canaux diplomatiques ou le soutien d'autres organisations (par exemple le CICR). Identifier les domaines dans lesquels une organisation pourrait envisager une campagne de plaidoyer avec d'autres, comme le bombardement d'infrastructures ou l'impunité des poursuites.
9. Pouvons-nous utiliser les données pour identifier un seuil de risque que notre organisation est prête à accepter ?		
Quels types de décisions ont été prises pendant la période analysée pour donner une indication du seuil de risque que l'organisation est prête à prendre ?	Pensez de façon critique à votre propre prise de décision concernant les risques de sécurité. Quels sont les principes et les seuils sur lesquels vous vous basez ? Entamez un dialogue avec d'autres membres du personnel de l'organisation et déterminez si vous utilisez les mêmes principes et seuils.	Recommander l'élaboration d'un seuil de risque clairement défini à communiquer au personnel.
Dans quelle mesure cette prise de décision était-elle cohérente entre différents contextes ?		
Y a-t-il une relation entre les incidents de sécurité signalés et les décisions spécifiques prises ?		