

GUIDE EBIOS RISK MANAGER

FICHE METHODE – Ateliers 1 et 3

EVALUER LA GRAVITE DES EVENEMENTS REDOUTES

Les fiches méthodes permettent aux responsables de la démarche d'analyse de risque d'identifier les points essentiels d'attention en fonction de la typologie du système d'information ou des concepts utilisés.

Elles n'ont pas vocation à remplacer les guides techniques de l'ANSSI ou les politiques de sécurité et les réglementations en vigueur qui doivent être appliquées.

QUELLES CATEGORIES D'IMPACTS FAUT-IL PRENDRE EN COMPTE ?

Les catégories ci-après peuvent servir de base pour identifier les impacts liés aux événements redoutés et faciliter l'évaluation de la gravité :

- impacts sur les missions et services de l'organisation ;
- impacts humains, matériels ou environnementaux ;
- impacts sur la gouvernance ;
- impacts financiers ;
- impacts juridiques ;
- impacts sur l'image et la confiance.

NOTE : selon le contexte, certaines catégories peuvent correspondre à des facteurs aggravants ou à des impacts indirects.

IMPACT	EXEMPLES (LISTE NON EXHAUSTIVE)
IMPACTS SUR LES MISSIONS ET SERVICE DE L'ORGANISATION	
CONSÉQUENCES DIRECTES OU INDIRECTES SUR LA RÉALISATION DES MISSIONS ET SERVICES	Incapacité à fournir un service, dégradation de performances opérationnelles, retards, impacts sur la production ou la distribution de biens ou de services, impossibilité de mettre en œuvre un processus clé.
IMPACTS HUMAINS, MATÉRIELS OU ENVIRONNEMENTAUX	
IMPACTS SUR LA SÉCURITÉ OU SUR LA SANTÉ DES PERSONNES CONSÉQUENCES DIRECTES OU INDIRECTES SUR L'INTÉGRITÉ PHYSIQUE DE PERSONNES	Accident du travail, maladie professionnelle, perte de vies humaines, mise en danger, crise ou alerte sanitaire.
IMPACTS MATÉRIELS DÉGÂTS MATÉRIELS OU DESTRUCTION DE BIENS SUPPORTS	Destruction de locaux ou d'installations, endommagement de moyens de production, usure prématurée de matériels.
IMPACTS SUR L'ENVIRONNEMENT CONSÉQUENCES ÉCOLOGIQUES À COURT OU LONG TERME, DIRECTES OU INDIRECTES	Contamination radiologique ou chimique des nappes phréatiques ou des sols, rejet de polluants dans l'atmosphère.

IMPACTS SUR LA GOUVERNANCE	
IMPACTS SUR LA CAPACITÉ DE DÉVELOPPEMENT OU DE DÉCISION CONSÉQUENCES DIRECTES OU INDIRECTES SUR LA LIBERTÉ DE DÉCIDER, DE DIRIGER, DE METTRE EN ŒUVRE LA STRATÉGIE DE DÉVELOPPEMENT	Perte de souveraineté, perte ou limitation de l'indépendance de jugement ou de décision, limitation des marges de négociation, perte de capacité d'influence, prise de contrôle de l'organisation, changement contraint de stratégie, perte de fournisseurs ou de sous-traitants clés.
IMPACTS SUR LE LIEN SOCIAL INTERNE CONSÉQUENCES DIRECTES OU INDIRECTES SUR LA QUALITÉ DES LIENS SOCIAUX AU SEIN DE L'ORGANISATION	Perte de confiance des employés dans la pérennité de l'organisation, exacerbation d'un ressentiment ou de tensions entre groupes, baisse de l'engagement, perte de sens des valeurs communes.
IMPACTS SUR LE PATRIMOINE INTELLECTUEL OU CULTUREL CONSÉQUENCES DIRECTES OU INDIRECTES SUR LES CONNAISSANCES NON-EXPLICITES ACCUMULÉES PAR L'ORGANISATION, SUR LE SAVOIR-FAIRE, SUR LES CAPACITÉS D'INNOVATION, SUR LES RÉFÉRENCES CULTURELLES COMMUNES	Perte de mémoire de l'entreprise (anciens projets, succès ou échecs), perte de connaissances implicites (savoir-faire transmis entre générations, optimisations dans l'exécution de tâches ou de processus), captation d'idées novatrices, perte de patrimoine scientifique ou technique, perte de ressources humaines clés.
IMPACTS FINANCIERS	
CONSÉQUENCES PÉCUNIAIRES, DIRECTES OU INDIRECTES	Perte de chiffre d'affaires, perte d'un marché, dépenses imprévues, chute de valeur en bourse, baisse de revenus, pénalités imposées.
IMPACTS JURIDIQUES	
CONSÉQUENCES SUITE À UNE NON-CONFORMITÉ LÉGALE, RÉGLEMENTAIRE, NORMATIVE OU CONTRACTUELLE	Procès, amende, condamnation d'un dirigeant, amendement de contrat.
IMPACTS SUR L'IMAGE ET LA CONFIANCE	
CONSÉQUENCES DIRECTES OU INDIRECTES SUR L'IMAGE DE L'ORGANISATION, LA NOTORIÉTÉ, LA CONFIANCE DES CLIENTS	Publication d'articles négatifs dans la presse, perte de crédibilité vis-à-vis de clients, mécontentement des actionnaires, perte de notoriété, perte de confiance d'usagers.

QUELLE ECHELLE DE GRAVITE UTILISER ?

Lorsque l'on crée une échelle de niveaux d'impacts, le principal enjeu réside dans le fait qu'elle soit comprise et utilisable par les personnes amenées à évaluer l'importance des conséquences d'un événement redouté. Il est conseillé de l'élaborer en concertation avec les personnes qui vont estimer ces niveaux – particulièrement les métiers – afin de faciliter son appropriation et la cohérence de la cotation. L'échelle de gravité à privilégier reste celle déjà mise en place (si elle existe) pour apprécier les risques de l'organisation dans le cadre d'une démarche globale de management du risque (incluant les risques financier, juridique, etc.). Le risque numérique doit en effet s'insérer dans la cartographie globale du risque. D'autre part, un certain nombre de réglementations sectorielles disposent d'échelles de niveaux d'impacts qu'il convient d'utiliser ou avec lesquelles il convient au moins d'être compatible.

Si vous ne disposez pas d'une telle échelle, établissez-en une avec les métiers dès le début de l'atelier dédié aux événements redoutés. Pour ce faire, vous pouvez utiliser et adapter l'échelle générique ci-après. Elle tient compte des impacts internes à l'organisation et d'éventuelles conséquences externes sur les écosystèmes.

NIVEAU DE L'ÉCHELLE	DÉFINITION
G5 CATASTROPHIQUE	Conséquences sectorielles ou régaliennes au-delà de l'organisation. Écosystème(s) sectoriel(s) impacté(s) de façon importante, avec des conséquences éventuellement durables. Et/ou : difficulté pour l'État, voire incapacité, d'assurer une fonction régalienne ou une de ses missions d'importance vitale. Et/ou : impacts critiques sur la sécurité des personnes et des biens (crise sanitaire, pollution environnementale majeure, destruction d'infrastructures essentielles, etc.).
G4 CRITIQUE	Conséquences désastreuses pour l'organisation avec d'éventuels impacts sur l'écosystème. Incapacité pour l'organisation d'assurer la totalité ou une partie de son activité, avec d'éventuels impacts graves sur la sécurité des personnes et des biens. L'organisation ne surmontera vraisemblablement pas la situation (sa survie est menacée), les secteurs d'activité ou étatiques dans lesquels elle opère seront susceptibles d'être légèrement impactés, sans conséquences durables.
G3 GRAVE	Conséquences importantes pour l'organisation. Forte dégradation des performances de l'activité, avec d'éventuels impacts significatifs sur la sécurité des personnes et des biens. L'organisation surmontera la situation avec de sérieuses difficultés (fonctionnement en mode très dégradé), sans impact sectoriel ou étatique.
G2 SIGNIFICATIVE	Conséquences significatives mais limitées pour l'organisation. Dégradation des performances de l'activité sans impact sur la sécurité des personnes et des biens. L'organisation surmontera la situation malgré quelques difficultés (fonctionnement en mode dégradé).
G1 MINEURE	Conséquences négligeables pour l'organisation. Aucun impact opérationnel ni sur les performances de l'activité ni sur la sécurité des personnes et des biens. L'organisation surmontera la situation sans trop de difficultés (consommation des marges).

L'usage d'une échelle à 4 ou 5 niveaux est guidé par la nécessité de mesurer des impacts très élevés qui correspondent à des crises majeures, voire une déstabilisation et une perte de résilience allant au-delà de la seule organisation concernée (exemples : paralysie ou forte dégradation de l'ensemble d'un secteur industriel, incapacité pour l'État d'assurer une fonction régalienne, crise sanitaire ou pollution majeure touchant une zone importante, compromission d'information hautement classifiée). Dans ce cas, une échelle à 5 niveaux est recommandée. Dans le cas contraire, 4 niveaux suffiront.

NOTE : l'estimation de l'importance des impacts doit être contextualisée, de telle sorte que les acteurs soient capables de distinguer les niveaux d'impacts de l'échelle. Une façon usuelle de procéder est d'appuyer d'exemples la description de chaque niveau.

Exemple d'échelle de gravité pour une activité de production industrielle

NIVEAU DE L'ÉCHELLE	CONSÉQUENCES SUR L'EXPLOITATION
G4 - CRITIQUE	Arrêt durable de l'exploitation nécessitant une intervention de maintenance.
G3 - GRAVE	Arrêt temporaire de l'exploitation puis reprise sous une procédure particulière (exemple : opérateur supplémentaire).
G2 - SIGNIFICATIVE	Poursuite de l'exploitation avec une action opérateur.
G1 - MINEURE	Poursuite de l'exploitation avec une alarme signalant le défaut.