MINISTÈRE
DES ARMÉES
Liberté
Égalité
Fraternité

GUIDE PRATIQUE ANALYSE DE RISQUES

Septembre
2023

La DPID et la DRSD vous présentent ce guide pratique d'analyse de risques conçu comme un outil destiné à vous accompagner dans la gestion efficace des menaces et des aléas auxquels vous pourriez être confrontés. Dans un monde en constante évolution, où les risques se multiplient et se complexifient, il est crucial de disposer de méthodes rigoureuses pour les évaluer, les comprendre et en atténuer les effets.

Ce guide est le fruit d'un travail conjoint de professionnels expérimentés dans le domaine de la gestion des risques au sein de la DPID et de la DRSD. Ce manuel didactique complet est destiné à vous fournir les connaissances nécessaires pour identifier, analyser les risques et adopter les mesures et postures efficaces de prévention et de protection au sein de votre organisation appartenant à la sphère défense, qu'elle soit militaire ou civile.

L'objectif principal de ce guide est de vous offrir une approche structurée et méthodique pour évaluer les risques potentiels et prendre des décisions éclairées. En suivant les étapes claires et les bonnes pratiques recommandées, vous serez en mesure de mettre en œuvre des stratégies adaptées au contexte singulier de votre organisation.

Au-delà des préconisations théoriques, ce guide vous propose également des exemples concrets, sous forme d'études de cas, et des outils pratiques pour faciliter votre apprentissage puis votre emploi. Vous trouverez des conseils sur la collecte des données, l'identification et la caractérisation des menaces et des aléas potentiels, l'évaluation des impacts, ainsi que sur les politiques de maîtrise des risques.

La gestion des risques au sein du ministère des Armées est une responsabilité partagée, et nous sommes convaincus que ce guide vous aidera à renforcer votre capacité à anticiper et à gérer les défis auxquels vous serez confrontés. Nous espérons que cet ouvrage vous accompagnera dans votre parcours vers une gestion proactive des risques.

Nous vous souhaitons une lecture enrichissante et fructueuse. Puissiez-vous utiliser ce guide pour renforcer votre résilience, assurer la pérennité de votre organisation et protéger vos intérêts, inamovibles.

Le général de corps d'armée Philippe Susnjara

Directeur du renseignement et de la sécurité de la défense

Le vice-amiral Denis Bertrand

Directeur de la protection des installations, moyens et activités de la défense, haut fonctionnaire correspondant de défense et de sécurité adjoint

PRÉFACE

Nous le savons plus que quiconque à la DRSD, à la DPID ainsi qu'au CDSE. Il y a une chose que le monde des armées et de la sécurité dans sa globalité partage avec celui de l'Entreprise : un amour peut-être un peu trop prononcé pour les sigles et les acronymes…

Néanmoins, à l'heure où je prends la plume pour préfacer ce guide pratique sur l'analyse des risques, un « substantif dont l'origine est un sigle, mais qui se prononce comme un mot ordinaire » me vient à l'esprit. Celui de VUCA, pour Volatility, Uncertainty, Complexity, Ambiguity. Cet acronyme résume un concept développé par l'US Army War College en 1991 pour redéfinir le contexte mondial à l'ère post-guerre froide. Un monde caractérisé par sa Volatilité, son Incertitude, sa Complexité et son Ambiguïté. Cette idée, pratiquement oubliée pendant trois décennies - celles de la mondialisation et de la numérisation « heureuses » - connait un regain d'intérêt depuis 2020 et la pandémie de COVID, mais dans le monde de l'Entreprise cette fois, où ce concept est désormais repris par les dirigeants exécutifs, les administrateurs et les théoriciens du management.

Le monde militaire inspire ainsi le monde de l'Entreprise – et inversement même si cette tendance peut encore se développer davantage -, ce n'est pas un fait nouveau. Ce guide pratique à destination des organisations du ministère des Armées et des entreprises de l'industrie de défense en est une nouvelle fois la preuve.

Dans un monde volatile, incertain, complexe et ambigu, les organisations doivent donc impérativement se préparer à toute éventualité, à « penser l'impensable et manager l'incertitude » afin de garantir la continuité de leur activité. Dans les entreprises, les directeurs sécurité-sûreté et leurs collaborateurs en sont les garants. Ils savent en effet mieux que quiconque traduire les effets de la crise en monnaie sonnante et trébuchante, en chiffre d'affaires, en EBITDA, en parts de marchés. Ils savent ainsi que leur donner les moyens de la « bien gérer », de la « bien anticiper » est un investissement à la rentabilité avérée, ne serait-ce qu'en prenant comme indicateur celui du « coût évité ». Ils savent donc combien de sa bonne gestion et, mieux encore, de son anticipation et de la juste analyse des risques (fondement de tout plan de gestion de crise et de continuité d'activité) peuvent dépendre la vie ou la mort de leur entreprise.

Ils savent enfin qu'il est fondamental, dans le cadre de ce que l'on pourrait appeler « la légitime défense économique », de partager les bonnes pratiques, de croiser les expertises et les savoir-faire.

C'est pourquoi ce manuel pragmatique, car agrémenté d'études de cas concrets et d'outils pratiques, s'appuyant sur l'expertise de la DRSD et de la DIPD est donc à mettre entre les mains de tous les professionnels de la gestion des risques, qu'ils soient militaires ou civils !

Stéphane Volant

Président du CDSE

INTRODUCTION : Généralités

L'AMBITION DE CE GUIDE

Ce guide vise à **accompagner les organisations du périmètre du ministère des Armées dans la mise en place d'un processus de management des risques** dans le cadre de la protection des installations, moyens et activités de la défense.

Ce guide a pour ambition de faciliter une démarche de management des risques, de délivrer des conseils méthodologiques, et de diffuser des bonnes pratiques. Il vise à mettre en cohérence le vocabulaire et les méthodologies existantes, dans un contexte où le ministère des Armées et le secteur privé sont amenés à renforcer la résilience de la Nation de manière complémentaire.

Ce guide est scindé en deux parties. La première développe une démarche « tous risques ». La seconde se concentre sur le « risque malveillance » visant le secret de la défense nationale.

La méthodologie a pour objectif d'**évaluer les risques auxquels les organisations sont exposées** à partir de l'étude des menaces et des aléas, en articulation avec le référentiel ministériel en vigueur. Sa finalité est d'identifier les priorités de traitement et les mesures de sécurité à mettre en œuvre pour maîtriser les risques dans une démarche d'amélioration continue.

La méthodologie privilégie une **approche ascendante** en partant du contexte de l'organisation jusqu'à l'étude des scénarios de menaces et d'aléas possibles. Elle vise à faire correspondre les scénarios élaborés à la réalité des organisations, à travers une étude de l'environnement à réaliser au commencement de la démarche.

POURQUOI RÉALISER UNE ANALYSE DE RISQUES ?

Les organisations, qu'elles soient publiques ou privées, sont de plus en plus confrontées à des risques dont la nature, la fréquence et la gravité ne cessent d'évoluer.

La survenance d'**un événement dommageable peut perturber considérablement une organisation et avoir des conséquences multiples sur les activités de la défense** :

- **internes**, dues aux pertes humaines, à la perte de l'outil de production, d'informations sensibles et classifiées, d'une capacité opérationnelle, etc. ;
- **externes**, dues à la dégradation de l'image de l'organisation, aux ruptures d'approvisionnement et de contrats, aux poursuites judiciaires, etc.

Les organisations ayant entrepris une démarche de management des risques sont plus résilientes face aux événements déstabilisants. Le propriétaire du risque est invité à **concevoir et conduire une stratégie de maîtrise des risques** pour réduire l'exposition de son organisation aux menaces et aux aléas. Cette stratégie vise à évaluer la criticité du risque de l'organisation, déterminer des priorités de traitement et réduire les risques par la mise en œuvre de mesures de sécurité.

Pour entreprendre une stratégie de maîtrise des risques, il convient de **disposer d'outils méthodologiques permettant d'évaluer les risques** en cohérence avec l'environnement de l'organisation. **Ce guide propose de suivre une démarche « tous risques », applicable à toutes menaces et à tous aléas, et adaptée au contexte du ministère des Armées.**

La méthode repose sur des outils de cotation dont le facteur gravité est pondéré au carré afin de souligner que l'impact d'un événement dommageable prévaut sur la probabilité qu'il se produise. **La matrice des risques est chiffrée pour permettre une analyse quantifiée et simplifiée.** Il est ainsi possible de hiérarchiser les risques, de les comparer et de les pondérer avec des critères évaluant les mesures de réduction des vulnérabilités de l'organisation. **La matrice des risques est facilement modulable,** de sorte que les organisations puissent l'adapter en fonction du seuil d'acceptation des risques déterminé par le propriétaire du risque conformément, le cas échéant, aux dispositions juridiques applicables.

INTRODUCTION : Méthodologie

PROCESSUS DU MANAGEMENT DES RISQUES

Le management des risques se définit, selon la norme ISO 31000, comme étant les activités coordonnées dans le but de diriger et piloter une organisation vis-à-vis d'un risque.

Le guide se fonde sur les principes de méthodes connues. La norme ISO 31000 fournit un cadre et des lignes directrices pour gérer toute forme de risque. La norme ISO 31010 décline les techniques d'appréciation du risque, utilisables par toute organisation, sans distinction de taille, d'activité ou de secteur. La série de normes ISO/IEC 27000 les décline pour le secteur de la sécurité de l'information.

La méthode permet de prendre en compte les risques d'origine cyber. Elle ne remplace pas EBIOS RM qui reste la méthode de référence pour les homologations de systèmes numériques, mais peut s'y substituer lorsque la situation s'y prête (par exemple pour définir les mesures de protection et de défense pour un système de systèmes dans le cadre d'un essai soumis à de nombreuses menaces physiques et numériques).

Le guide s'inscrit dans une démarche de renforcement de la résilience du ministère des Armées et de son périmètre. L'arrêté du 2 juillet 2018 approuve une méthode d'analyse des risques applicable pour le secteur des activités d'importance vitale. Le secteur de la continuité d'activité peut s'appuyer sur le guide élaboré en 2022 par le Secrétariat général de la défense et de la sécurité nationale (SGDSN).

Le guide propose de suivre un **processus de management des risques** composé de quatre phases itératives :

Figure 1. Illustration du processus de management des risques proposé par le guide.

ANALYSE DE RISQUES

L'analyse de risques s'insère dans le processus de management des risques. Elle correspond aux phases d'appréciation et d'évaluation des risques.

L'analyse de risques vise à :
- étudier l'environnement et le contexte ;
- identifier les valeurs de l'organisation ;
- étudier les menaces et les aléas de toutes natures ;
- identifier les scénarios de risques ;
- cartographier les risques en fonction de critères de probabilité et de gravité ;
- évaluer les risques en fonction des obligations de sécurité de l'organisation ainsi que du contexte et des enjeux de ses activités.

L'analyse de risques permet de déterminer les priorités de traitement parmi les scénarios de menaces et d'aléas. Le plan de traitement s'insère dans une démarche d'amélioration continue par la surveillance du contexte des risques ainsi que par le réexamen et le contrôle des mesures de sécurité.

GUIDE PRATIQUE D'ANALYSE DE RISQUES

Partie 1

SOMMAIRE : Une démarche didactique et itérative

La méthodologie présentée consiste à procéder à une analyse didactique, séquencée en onze étapes, ayant pour but d'évaluer l'exposition des valeurs de l'organisation aux menaces et aux aléas, afin de décider d'un plan de traitement des risques.
Cette méthodologie n'a aucun caractère obligatoire. Ainsi, les entités disposant d'une autre méthode d'analyse de risques satisfaisante peuvent ne pas recourir à cette méthode.

APPRÉCIATION DES VALEURS ET DE L'ENVIRONNEMENT

La **phase d'appréciation des valeurs et de l'environnement** se déroule en deux étapes. Elle correspond à réaliser un inventaire de toutes les données d'entrée de mon organisation nécessaires à la phase d'évaluation du risque.

ÉVALUATION DES RISQUES

La **phase d'évaluation des risques** se déroule en six étapes. Elle correspond à réaliser une cotation et une cartographie du niveau de criticité des scénarios de risques auxquels mon organisation est exposée.

MAÎTRISE ET TRAITEMENT DES RISQUES

La **phase de maîtrise et de traitement des risques** se déroule en deux étapes. Elle correspond à déterminer des mesures de traitement à partir des priorités établies lors de la phase d'évaluation des risques.

SURVEILLANCE, CONTRÔLE ET RÉEXAMEN DES RISQUES

La **phase de surveillance, de contrôle et de réexamen des risques** correspond à une démarche d'amélioration continue des mesures du plan de traitement.

ÉTAPE 1 J'analyse l'environnement de mon organisation

En préliminaire de l'analyse de risques, je dois collecter toutes les données, informations utiles et nécessaires afin d'appréhender la globalité de l'écosystème interne et externe de l'organisation. Je réemploierai ces données d'entrée tout au long de l'analyse.

L'environnement d'une organisation correspond au contexte externe et interne dans lequel l'organisme cherche à définir et atteindre ses objectifs.

COMPRENDRE MON ENVIRONNEMENT

Afin d'initier un processus de management du risque, je dois comprendre l'**environnement externe et interne** dans lequel opère mon organisation. L'analyse doit refléter l'environnement spécifique de l'activité à laquelle le processus de management du risque s'applique.

La compréhension du contexte est importante car le management du risque a lieu dans le contexte des objectifs et des activités de l'organisation. Il s'agit d'un processus dynamique et itératif, qu'il convient d'adapter aux besoins et à la culture de l'organisation.

ÉTUDIER LE CONTEXTE INTERNE

Le **contexte interne** correspond à l'environnement interne dans lequel l'organisation cherche à atteindre ses objectifs.

J'analyse l'environnement de mes installations à partir des informations sur le contexte des moyens et des activités de mon organisation. Je peux analyser les informations générales applicables à tout type d'analyse de risque, ainsi que les informations spécifiques à une analyse de la malveillance.

Je peux étudier le contexte interne de mon organisation à partir de l'analyse des éléments ci-après.

CONTEXTE INTERNE

Structure et accessibilité

Plan de masse du site, informations générales sur la périphérie, la périmétrie et la volumétrie du site, emprises annexes, utilités et fluides.

Issues principales et secondaires, issues de secours, ouvrants, servitudes et accès adjacents, accessibilité, transports, etc.

Organisation

Gouvernance, responsabilités, rôles, processus de prise de décision, interdépendances, etc.

Organigramme fonctionnel, nombre et répartition des effectifs, affectation des locaux, habitudes et horaires de présence sur le site, etc.

Activités et objectifs

Description du secteur d'activité, flux et processus, sous-traitance, clients, fournisseurs.

Stratégies pour atteindre les objectifs, politiques internes et lignes directrices, valeurs, culture, etc.

Information et communication

Techniques d'information et de communication, systèmes et flux d'information, installations de télécommunication et sauvegardes, etc.

Culture interne, perception de l'organisation et valeurs, etc.

Capacités et ressources

Stock de matériels, connaissances et ressources immatérielles, temps, métiers, processus, systèmes, technologies, etc.

Sûreté et sécurité

Typologie de l'installation et protection juridique, obligations légales et/ou réglementaires applicables.

Moyens et dispositifs de protection mécanique et physique (clôtures, camouflage, obstacles, etc.), électronique (vidéosurveillance, contrôle d'accès, télésurveillance), humain.

Historique, plans de sécurisation (PCA, sauvegarde, sauvetage, survie) et documents (main courante, journaux d'événements), mesures compensatoires, consignes de sécurité.

ÉTUDIER LE CONTEXTE EXTERNE

Le **contexte externe** correspond à l'environnement externe dans lequel l'organisation cherche à atteindre ses objectifs.

Je peux étudier le contexte externe de mon organisation à partir de l'analyse des éléments ci-après.

CONTEXTE EXTERNE

Politique

Stabilité des institutions et du gouvernement, conflits internes et externes, etc.

Économique

Niveau de revenus et d'éducation, taux de chômage, d'inflation, de pauvreté, démographie etc.

Social

Population au voisinage, conflits sociaux, niveau d'activisme, communautés, image et notoriété de l'organisation, etc.

Malveillances

Présence policière, niveau d'atteinte aux biens et aux personnes, groupes criminels ou terroristes, etc.

Relations contractuelles

Relations avec les parties prenantes externes (dont sous-traitants), leurs perceptions et leurs valeurs.

Environnemental

Exposition à un aléa naturel (inondation, séisme, volcanisme, etc.) ou industriel et technologique (installation SEVESO, etc.), circulation et flux.

Le contexte externe vise à mieux comprendre l'environnement extérieur de mon organisation afin de recueillir des données d'entrée qui me seront utiles lors de la phase d'analyse de risques. En particulier, l'étude du contexte externe me permettra de m'aider à coter la probabilité des scénarios (**ÉTAPE 4**).

Néanmoins, l'étude du contexte externe ne correspond pas au recensement des menaces et des aléas qui sont susceptibles d'affecter mon organisation. Pour cela, je peux me référer aux catalogues existants relatifs aux menaces et aux aléas.

ÉTAPE 1

EXEMPLE BASE NAVALE FICTIVE, exemple décliné tout au long du guide

L'exemple considère une **base navale fictive**, localisée sur une façade maritime du territoire et constituée d'infrastructures terrestres et maritimes. Limitrophe d'une ville moyenne, la base s'étend sur plusieurs kilomètres le long d'une rade. Elle abrite une flotte de surface, des installations de soutien, et plusieurs milliers de personnels militaires et civils (dont industriels de défense et sous-traitants).
La base navale a pour **activités principales** : le soutien logistique et portuaire aux bâtiments de surface, le soutien de l'homme, et la surveillance maritime de la zone. Des **activités de support** concourent à la réalisation des objectifs : moyens portuaires (remorquage, maintenance, etc.), médicaux (centre médical, laboratoire, etc.), et de soutien (logement, restauration, etc.).

ÉTUDIER LE CONTEXTE INTERNE

Les éléments de contextualisation de l'environnement interne recensés ci-dessous sont non exhaustifs et sont proposés à titre d'illustration pour chaque item.

Structure et accessibilité

Configuration du site :
- superficie de 150 hectares, limitrophe à l'ouest avec une ville de taille moyenne (20 000 habitants) et un port civil enserre au sud les installations appartenant en pleine propriété à un industriel de défense ;
- 3 accès dont 1 principal (à l'ouest, port civil) et 2 secondaires (au sud, installations de l'industriel / à l'est, livraisons) ;
- 1 bassin pour les navires en stationnement, 1 bassin pour les navires en maintenance, 1 jetée pour l'appontement ;
- 1 laboratoire d'analyse et de surveillance, 3 ateliers, 2 bâtiments administratifs, 1 centre médical, logements, 2 entrepôts.

Accessibilité : au nord, l'accès principal est relié à une route départementale, aux transports en commun (bus) , et dédié à l'accès du personnel et des visiteurs. Au sud, un accès secondaire aux entrepôts et aux installations de l'industriel. À l'est, un accès secondaire assure l'approvisionnement en fret et les livraisons.

Utilités et fluides : combustible inflammable et hydrocarbures (carburants, huiles), matières explosives (munitions, dépôts de munitions), gaz (réservoirs, réseau de gaz naturel), eau, électricité, ventilation, compresseurs, chauffage, déchets industriels, etc.

Organisation

Organisation fonctionnelle générale :
- commandant de la base navale, responsable de la défense et sécurité, assisté d'un commandant en second ;
- division « activités » ;
- division « affaires générales » ;
- division « affaires industrielles ».

Répartition des effectifs :
5000 effectifs permanents (militaires et civils, industriels et sous-traitants, familles) :
- industriel (1700 employés civils + 300 sous-traitants), entreprises civiles en sous-traitance (300 employés) ;
- 2500 militaires et civils de la défense (unités et formation à terre + unités navigantes), familles logeant sur place (200 personnes).

Activités et objectifs

Missions principales :
- coordination des activités portuaires industrielles et militaires de la façade maritime ;
- surveillance maritime ;
- soutien logistique dont MCO des navires ;
- soutien de l'homme, formation.

Objectif principal : préparer les forces et assurer la disponibilité du matériel en vue de leur emploi opérationnel.

Information et communication

La base navale dispose de :

Systèmes d'information : postes Internet, postes Intradef, postes Intraced, applications métiers, etc.

Systèmes de communication : messagerie DR NEMO, messagerie ISIS, un TEOREM, radars, etc.

Culture, perceptions et valeurs : partenariats avec des établissements d'enseignement pour le recrutement, organisation d'événements institutionnels et de promotion de la Marine nationale auprès du public.

Capacités et ressources

La base navale dispose de :

Matériels : bâtiments de surface (frégates multi-missions, remorqueurs, etc.), armes de combat et munitions, etc.

Stocks : politique de gestion, entrepôts, inventaires réguliers, réapprovisionnement.

Personnels : militaires (officiers, officiers mariniers) et civils de la défense (fonctionnaires et contractuels), employés des industriels et sous-traitants, fournisseurs, stagiaires, visiteurs occasionnels.

Informations : informations et supports classifiés (ISC) numériques et papier, documents non sensibles, documents administratifs, base de données, savoir-faire en matière de technologie navale, méthodologie de travail, code source informatique, etc.

Technologies et systèmes : développement de l'IA, systèmes de combat, systèmes embarqués de surveillance et de transmission, laboratoire d'analyse, etc.

Sûreté et sécurité

Protection juridique : située en Zone protégée (ZP) et répertoriée Installation militaire de sensibilité haute (IMSH).

Historique des sinistres et incidents : selon le journal des événements, la base navale fait l'objet de repérages réguliers (depuis la terre et le long de sa façade maritime) et de pertes ponctuelles de matériels non sensibles.

Moyens de protection : la base navale dispose

- de moyens techniques de surveillance (vidéo, radar, sonar), de contrôle d'accès et de détection d'intrusion ;
- d'une surveillance humaine par une société privée (filtrage, gardiennage, levée de doute, intervention interne) et par des fusiliers marins ;
- de protection physique (sas, clôture, mur d'enceinte, barrière escamotable, barrière maritime, etc.) ;
- de dispositions organisationnelles (permanence de la chaîne de commandement de protection, plan NRBC, plan de protection du site, etc.).

ÉTUDIER LE CONTEXTE INTERNE

Politique

Le pays d'implantation de la base est caractérisé par :

- une démocratie libérale et des institutions stables ;
- un temps de paix sur le territoire national, une instabilité géopolitique (conflits internationaux) ;
- un engagement dans plusieurs OPEX.

Économique

Le territoire d'implantation de la base navale se caractérise par :

- un niveau de revenus et un taux de chômage moyen, une baisse de la démographie ;
- une concurrence industrielle avec l'étranger dans le secteur de l'armement et de l'énergie.

Social

Le territoire d'implantation de la base navale se caractérise par :

- un activisme régional (indépendantistes, écologistes) et des conflits sociaux (manifestations syndicales régulières) ;
- une présence au sein du territoire d'expatriés chinois et russes, d'étudiants étrangers spécialisés en ingénierie et en intelligence artificielle.

Malveillances

Le contexte de sécurité intérieure de la base navale est :

- une gendarmerie maritime présente sur la base, une caserne de pompiers à proximité (- de 5 km) ;
- une Zone de sécurité prioritaire (ZSP) à proximité, une délinquance locale modérée, une augmentation du nombre d'atteintes aux biens (statistiques 2022).

Relations contractuelles

La base navale détient des relations contractuelles avec :

- un industriel de défense implanté au sein de la base (infrastructures et personnels), concourant aux activités de maintenance et de recherche ;
- des sous-traitants de l'industriel ;
- des sociétés de gardiennage, de restauration et d'entretien des locaux de la base.

Environnemental

La base navale est exposée à :

- des submersions marines, vents ;
- un niveau de sécheresse modéré ;
- un niveau de sismicité modéré ;

La base navale est située à 15 km d'une usine de combustibles classée Seveso seuil haut.

PAGE DE NOTES

ÉTAPE 2 J'identifie les valeurs de mon organisation

Procéder à l'inventaire des valeurs que possède mon organisation me permettra d'apprécier les actifs pouvant être considérés comme prioritaires. Pour cela, je peux mesurer leur attractivité afin de déterminer au mieux le niveau de criticité de chaque scénario.

Une valeur est un bien, une personne, une information matérielle ou immatérielle, un savoir-faire, que détient un organisme et qui revêt un caractère précieux, voire indispensable pour son activité, son fonctionnement, sa pérennité, et vulnérable du fait de son prix, de son attrait commercial, de son coût de fabrication, de son délai de remplacement ou de son caractère unique.

IDENTIFIER LES VALEURS

Afin de recenser les valeurs, je dois considérer tous les actifs ayant de la valeur pour mon organisation et nécessitant une protection. Une cible est une valeur qui représente une forte attractivité pour un auteur de malveillance.

Les cibles correspondent à toutes les installations moyens, activités, personnes, systèmes d'information et de communication, flux dont l'atteinte, la perte, le vol, la destruction ou l'endommagement sont susceptibles de diminuer la disponibilité des moyens de la défense ou d'impacter son intégrité.

Parmi elles, **je dois recenser en particulier les actifs ayant une valeur critique pour mon organisation**. Il est possible de s'appuyer sur les catégories de valeurs ci-dessous pour procéder à un inventaire non exhaustif.

Ressources humaines

Personnel interne disponible, personnes détenant un savoir-faire stratégique, compétences, motivation, personnel externe (client, fournisseur, stagiaire), etc.

Ressources intellectuelles

Données internes, savoir et savoir-faire détenus, informations sensibles et ISC, technologies, PPST, RH, etc.

Systèmes d'informations

Serveurs, réseaux, applications, logiciels, télécommunication, etc.

Image

Réputation, confidentialité, stratégie.

Infrastructures

Bâtiments, entrepôts, bureaux, point névralgique, etc.

Prestations externes

Sous-traitants, partenaires critiques, fournisseurs, matières premières, énergie, etc.

Matériels et capacités

Equipements, liquidités et trésorerie, stocks intermédiaires et de produits finis, matériels, outils spéciaux, machines, services, etc.

Transport

Énergies, fluides, déchets, rebus, etc.

ESTIMER LEUR ATTRACTIVITÉ

Pour les menaces, je peux estimer l'attractivité de chaque valeur à la malveillance en utilisant l'échelle de critères suivante.

CRITÈRE DE CARACTÉRISATION	1	2	3	4
ATTRACTIVITÉ DE LA VALEUR	La cible n'est pas attractive	La cible est peu attractive	La cible est attractive et/ ou connue de plusieurs personnes	La cible est très attractive et/ ou connue de nombreuses personnes

ÉTAPE 2

EXEMPLE BASE NAVALE FICTIVE

IDENTIFIER LES VALEURS ET ESTIMER LEUR ATTRACTIVITÉ

À partir de l'analyse du contexte interne de mon organisation (**ÉTAPE 1**), j'identifie mes valeurs critiques.
Pour les menaces, je peux évaluer l'attractivité de chacune de mes valeurs sur une cotation de 1 à 4.

***Note** : pour le besoin de l'exemple, les seize valeurs recensées ci-dessous sont non exhaustives et sont proposées à titre d'illustration pour chaque item.*

N°	VALEURS	ATTRACTIVITÉ
	Ressources humaines	
1	Autorité militaire de haut rang sur la base	4
2	Ingénieurs spécialisés dans l'étude des systèmes de combat	3
	Ressources intellectuelles	
3	ISC papier protégée dans les coffres forts des bureaux	3
4	Organigramme de la base navale	1
	Systèmes d'informations	
5	Téléphone professionnel	3
6	Local hébergeant des serveurs informatiques Intradef	2
	Image	
7	Capacité de recrutement et attractivité auprès des jeunes	1
8	Attractivité des événements dédiés au rayonnement	2
	Infrastructures	
9	Quai d'embarquement/de stationnement des navires	4
10	Bureaux administratifs et de soutien	2
	Prestations externes	
11	Fournisseur d'électricité	4
12	Sous-traitant réalisant la restauration collective	2
	Matériels et capacités	
13	Frégate multi-missions en indisponibilité pour réparation	3
14	Engin de chantier stationné dans un entrepôt de stockage	1
	Transport	
15	Cuves de stockage du pétrole approvisionnant les navires	2
16	Livraison de produits alimentaires par un prestataire	2

ÉTAPE 3 J'étudie les scénarios crédibles pour mon organisation

Afin de dresser la liste des menaces et des aléas auxquels mon organisation est exposée, je peux sélectionner les scénarios les plus pertinents à partir du catalogue des menaces et des aléas avant de pouvoir envisager des actions de réduction du risque.

Pour sélectionner les scénarios pertinents, je peux utiliser le catalogue ministériel des menaces et des aléas qui constitue le référentiel des menaces et des aléas concernant les installations, moyens et activités relevant de la responsabilité du ministère des Armées.
En outre, je peux (ou je dois) utiliser d'autres catalogues existants pour compléter l'analyse et l'adapter à mon organisation, conformément, le cas échéant, aux obligations légales et réglementaires applicables compte tenu du statut du site et/ou de la nature de l'activité menée.

Une menace est une manifestation signifiant une intention hostile, le projet de nuire. Elle varie en fonction de son auteur, de ses ressources, de son degré de motivation, mais aussi des capacités et vulnérabilités de l'entité menacée.

Un aléa est la manifestation d'un phénomène naturel ou anthropique. Il exclut toute intention malveillante.

CONFRONTER MES VALEURS AVEC LES MENACES ET ALÉAS

L'appréciation des risques doit permettre à mon organisation de prendre conscience et d'apprécier correctement les menaces et les aléas les plus significatifs auxquels elle est exposée.

Je peux confronter les valeurs que j'ai identifiées durant l'ÉTAPE 2 avec les sous-catégories de menaces et d'aléas du catalogue ministériel ci-dessous :

CAT.1. MENACES DIRECTES	
CAT.1.1	Agression directe
CAT.1.2	Terrorisme
CAT.1.3	Espionnage
CAT.1.4	Sabotage
CAT.1.5	Subversion
CAT.1.6	Crime organisé
CAT.1.7	Acte de malveillance

CAT.2. MENACES INDIRECTES	
CAT.2.1	Troubles sociétaux internes graves
CAT.2.2	Menace économique
CAT.2.3	Phénomène migratoire massif extérieur
CAT.2.4	Dommage collatéral causé par un incident ou un conflit extérieur

CAT.3. ALÉAS	
CAT.3.1	Aléa naturel
CAT.3.2	Aléa ou événement sanitaire
CAT.3.3	Aléa technologique ou industriel

Pour chaque valeur, **j'étudie si celle-ci est susceptible d'être visée par une menace ou d'être exposée à un aléa**. Pour cela, je peux utiliser un tableau de croisement tel que le modèle ci-après.

Enfin, **je calcule le nombre total de combinaisons** de valeurs identifiées comme étant susceptibles d'être visées par une menace ou d'être exposées à un aléa.

SÉLECTIONNER LES SCÉNARIOS LES PLUS PERTINENTS

A partir de la confrontation de mes valeurs aux sous-catégories du catalogue, **je détermine le nombre de scénarios que mon organisation doit prendre en compte**. Le nombre total de combinaisons représente le nombre total de scénarios que je dois considérer dans l'analyse.

À partir du catalogue ministériel, **je peux rédiger un scénario pertinent pour chaque combinaison**. je dois tenir compte de la configuration de mon installation, du contexte de mes valeurs, et de mes connaissances sur l'environnement de mes installations, moyens et activités.

Afin de m'aider à rédiger des scénarios pertinents, je peux utiliser les typologies du catalogue ministériel en m'appuyant sur le guide d'utilisation du document.

Figure 2. Illustration des typologies du catalogue ministériel des menaces et des aléas.

La typologie des **vecteurs** est applicable uniquement pour les scénarios de menace.

Je peux constituer des scénarios combinant plusieurs modes opératoires pour souligner la concomitance des menaces et des aléas et pour identifier des effets en cascade.

SYNTHÈSE DES TYPOLOGIES DU RÉFÉRENTIEL MINISTÉRIEL

Les scénarios faisant l'objet de l'analyse de risques peuvent être sélectionnés à partir du **référentiel ministériel des menaces et des aléas**. Le référentiel catégorise les menaces et les aléas dans six typologies de référence illustrées ci-après.

Pour les besoins de la méthodologie, l'**ÉTAPE 3** précise la manière d'utiliser les typologies pour en déduire des scénarios applicables à l'environnement de mon organisation.

EXTRACTION DU CATALOGUE MINISTÉRIEL 2023 DES MENACES ET DES ALÉAS

SOUS-CATÉGORIES DES MENACES ET DES ALÉAS	
N°	Typologie
CAT.1	MENACES DIRECTES
CAT.1.1	Agression directe
CAT.1.2	Terrorisme
CAT.1.3	Espionnage
CAT.1.4	Sabotage
CAT.1.5	Subversion
CAT.1.6	Crime organisé
CAT.1.7	Acte de malveillance
CAT.2	MENACES INDIRECTES
CAT.2.1	Troubles sociétaux internes graves
CAT.2.2	Menace économique
CAT.2.3	Phénomène migratoire massif extérieur
CAT.2.4	Conséquences collatérales d'un incident ou un conflit extérieur
CAT.3	ALÉAS
CAT.3.1	Aléa naturel
CAT.3.2	Aléa ou événement sanitaire
CAT.3.3	Aléa technologique ou industriel

MILIEUX ET CHAMPS	
N°	Typologie
MIL.1	Milieu air
MIL.2	Milieu terre
MIL.3	Milieu mer
MIL.4	Milieu spatial
MIL.5	Champ numérique
MIL.6	Champ électromagnétique
MIL.7	Champs économique, financier et/ou juridique
MIL.8	Champ informationnel

ACTEURS	
N°	Typologie
ACT.1	ACTEURS ÉTATIQUES
ACT.1.1	État étranger
ACT.1.2	Coalition
ACT.1.3	Milice
ACT.1.4	Proxy
ACT.2	ACTEURS NON ÉTATIQUES A MOTIVATION IDÉOLOGIQUE OU RELIGIEUSE
ACT.2.1	Terroriste/ groupe terroriste
ACT.2.2	Extrémiste/ groupe extrémiste
ACT.2.3	Activiste/ groupe activiste
ACT.3	AUTEURS ISOLÉS OU GROUPES D'INDIVIDUS NON ORGANISÉS
ACT.3.1	Criminel
ACT.3.2	Délinquant
ACT.3.3	Groupe anomique
ACT.3.4	Déséquilibré
ACT.4	ACTEURS ÉCONOMIQUES
ACT.4.1	Entreprise concurrente
ACT.4.2	Organisation criminelle
ACT.4.3	Société militaire privée
ACT.4.4	Lobby
ACT.5	ÉLÉMENTS DÉCLENCHEURS DES ALÉAS
ACT.5.1	Dérèglement climatique
ACT.5.2	Evénement naturel
ACT.5.3	Evénement accidentel
ACT.5.4	Evénement anthropique (résultant d'une activité humaine)

CIBLES	
N°	Typologie
CIB.1	INSTITUTIONS
CIB.1.1	Ministère des Armées
CIB.1.2	Industrie de défense
CIB.1.3	Partenaire de la défense hors BITD
CIB.2	PERSONNES
CIB.2.1	Personnel
CIB.2.2	Haute autorité/personne publique
CIB.2.3	Famille et proches du personnel
CIB.3	BIENS MATÉRIELS ET IMMATÉRIELS
CIB.3.1	Installation
CIB.3.2	Equipement
CIB.3.3	Composant/ point névralgique
CIB.3.4	Domaine/emprise
CIB.3.5	Information/ support sensible, protégé ou classifié
CIB.3.6	Potentiel scientifique et technique de la Nation
CIB.3.7	Système d'information et de communication
CIB.3.8	Réputation
CIB.4	ACTIVITÉS
CIB.4.1	Politique de défense du ministère des Armées
CIB.4.2	Fonctions opérationnelles d'une industrie de défense
CIB.4.3	Fonctions support
CIB.4.4	Activités clés à l'échelle nationale/ internationale

MODES OPÉRATOIRES DES MENACES ET TYPES DE MANIFESTATION DES ALÉAS	
N°	Typologie
MOP.1	ACTIONS DE COMMUNICATION
MOP.1.1	Manifestation/ grève
MOP.1.2	Fausse alerte
MOP.1.3	Diffusion d'une information ou d'un support/ compromission
MOP.2	ACTIONS DE DISSIMULATION
MOP.2.1	Piégeage
MOP.2.2	Leurrage
MOP.2.3	Usage de faux
MOP.2.4	Usurpation de titres ou de droits
MOP.3	ACTIONS DE RENSEIGNEMENT
MOP.3.1	Repérage
MOP.3.2	Espionnage
MOP.4	ACTIONS D'INFLUENCE
MOP.4.1	Lutte informationnelle
MOP.4.2	Manipulation/ intimidation d'une personne
MOP.4.3	Instrumentalisation des règles juridiques
MOP.4.4	Déstabilisation économique
MOP.5	ACTIONS D'INTRUSION
MOP.5.1	Entrisme
MOP.5.2	Intrusion physique
MOP.5.3	Cyberattaque suivant les phases de la *kill chain*
MOP.5.4	Débauchage du personnel
MOP.6	ATTEINTES AVEC ENGAGEMENT ARMÉ POSSIBLE
MOP.6.1	Atteinte à une personne
MOP.6.2	Dégradation/ destruction
MOP.6.3	Appropriation frauduleuse
MOP.6.4	Détournement
MOP.6.5	Assistance par un moyen robotique/IA
MOP.6.6	Programmation
MOP.6.7	Manœuvre de perturbation/ obstruction
MOP.7	ATTAQUES AVEC ENGAGEMENT ARMÉ
MOP.7.1	Attaque suicide
MOP.7.2	Exposition aux lasers/armes à énergie dirigée
MOP.7.3	Agression électromagnétique intentionnelle
MOP.7.4	Incorporation/ dispersion/ radiation de matières dangereuses
MOP.7.5	Emploi d'armes, munitions, missiles, explosifs, grenades, mines
MOP.7.6	Attaque nucléaire
TMA.8	TYPES DE MANIFESTATION DES ALÉAS NATURELS
TMA.8.1	Evénement hydrologique
TMA.8.2	Evénement géologique
TMA.8.3	Evénement météorologique
TMA.8.4	Incendie d'origine naturelle
TMA.9	TYPES DE MANIFESTATION DES ALÉAS SANITAIRES
TMA.9.1	Contamination
TMA.9.2	Infection
TMA.9.3	Pollution
TMA.9.4	Intoxication
TMA.10	TYPES DE MANIFESTATION DES ALÉAS TECHNOLOGIQUES OU INDUSTRIELS
TMA.10.1	Accident
TMA.10.2	Défaillance d'un réseau de fluides/d'énergie
TMA.10.3	Incendie d'origine technologique/ industrielle

VECTEURS	
N°	Typologie
VEC.1	AÉRONEFS ET ENGINS SPATIAUX CIVILS OU MILITAIRES
VEC.1.1	Aéronef motorisé à voilure fixe
VEC.1.2	Aéronef motorisé à voilure tournante
VEC.1.3	Drone aérien
VEC.1.4	Aéronef non motorisé
VEC.1.5	Aérostat
VEC.1.6	Engin aérospatial
VEC.1.7	Engin/objet spatial
VEC.2	VÉHICULES TERRESTRES CIVILS OU MILITAIRES
VEC.2.1	Véhicule terrestre civil
VEC.2.2	Véhicule militaire blindé de combat
VEC.2.3	Véhicule militaire léger ou moyen
VEC.2.4	Véhicule militaire d'artillerie
VEC.2.5	Véhicule et équipement militaire du génie
VEC.2.6	Véhicule militaire logistique
VEC.2.7	Robot/drone terrestre
VEC.3	NAVIRES CIVILS OU MILITAIRES
VEC.3.1	Navire civil de surface ou sous-marin
VEC.3.2	Bâtiment militaire de surface ou amphibie
VEC.3.3	Sous-marin militaire
VEC.3.4	Drone naval
VEC.4	ARMES
VEC.4.1	Arme à feu collective
VEC.4.2	Arme à feu individuelle
VEC.4.3	Arme de force intermédiaire
VEC.4.4	Arme blanche
VEC.4.5	Arme par destination
VEC.4.6	Arme à énergie dirigée
VEC.5	MUNITION, MISSILE, EXPLOSIF, GRENADE, MINE
VEC.5.1	Munition
VEC. 5.2	Missile/ torpille/ bombe
VEC.5.3	Explosif
VEC.5.4	Grenade
VEC.5.5	Mine
VEC.6	NRBC
VEC.6.1	Énergie nucléaire
VEC.6.2	Matière radioactive ou source radiologique
VEC.6.3	Agent biologique
VEC.6.4	Produit chimique
VEC.7	MOYENS NUMÉRIQUES OU TECHNIQUES
VEC.7.1	Système d'information
VEC.7.2	Système de communication
VEC.7.3	Système de captation de données
VEC.7.4	Support amovible/ périphérique
VEC.7.5	Faille du réseau
VEC.7.6	Faille logicielle
VEC.7.7	Hameçonnage
VEC.7.8	Bot
VEC.7.9	Troll / Usine à trolls
VEC.7.10	Deep fake
VEC.7.11	Objet connecté
VEC.7.12	Brouilleur électronique
VEC.8	TECHNOLOGIES ÉMÉRGENTES
VEC.8.1	Intelligence artificielle
VEC.8.2	Technologie quantique
VEC.9	MOYENS JURIDIQUES, FINANCIERS, HUMAINS
VEC.9.1	Moyen juridique
VEC.9.2	Moyen financier/ économique
VEC.9.3	Moyen humain

ÉTAPE 3

EXEMPLE BASE NAVALE FICTIVE

CONFRONTER MES VALEURS AVEC LES MENACES ET ALÉAS

1. Je confronte les valeurs critiques que j'ai identifiées durant l'**ÉTAPE 2** avec les menaces et aléas susceptibles de les viser ou les affecter. Pour cela, je peux étudier chaque valeur avec les sous-catégories du catalogue ministériel à travers le tableau de croisement ci-après.
2. Je coche la case dès lors que ma valeur étudiée peut être visée ou affectée par une sous-catégorie de menaces ou d'aléas.

VALEURS / SOUS-CATÉGORIES		N°1	N°3	N°5	N°7	N°9	N°11	N°13	N°15
CAT.1.1	Agression directe					X		X	
CAT.1.2	Terrorisme	X				X	X		X
CAT.1.3	Espionnage	X	X	X		X	X	X	
CAT.1.4	Sabotage		X	X		X	X	X	X
CAT.1.5	Subversion	X			X				
CAT.1.6	Crime organisé			X		X		X	X
CAT.1.7	Acte de malveillance	X	X	X		X	X	X	X
CAT.2.1	Troubles sociétaux internes graves	X			X	X			X
CAT.2.2	Menace économique						X		
CAT.2.3	Phénomène migratoire massif extérieur	X			X	X	X		X
CAT.2.4	Dommage collatéral (conflit ext. ou incident)				X		X		
CAT.3.1	Aléa naturel	X				X			X
CAT.3.2	Aléa ou événement sanitaire	X							X
CAT.3.3	Aléa technologique ou industriel	X				X			X
SOUS-TOTAUX		10	3	4	4	10	7	5	9
TOTAL		51 COMBINAISONS DE SCÉNARIOS							

Avertissement *: Toutes les valeurs critiques identifiées à l'étape 2 n'ont pas été reprises dans le tableau pour ne pas alourdir l'exposé.*

Lecture *: Une autorité militaire de haut rang présente sur la base (Valeur N°1) est susceptible d'être visée par un scénario relatif au Terrorisme (sous-catégorie CAT.1.2 de menace ou d'aléa).*

SÉLECTIONNER LES SCÉNARIOS LES PLUS PERTINENTS

1. À partir du tableau de croisement, je recense toutes les combinaisons de valeurs et de sous-catégories de menaces et d'aléas que j'ai identifiées.
2. À partir des typologies du catalogue ministériel, je peux rédiger un scénario pertinent pour chaque combinaison.

***Note** : pour le besoin de l'illustration de l'exemple, **3 scénarios seront étudiés dans l'ensemble du guide** parmi les 51 combinaisons possibles.*

COMBINAISON VALEUR / SOUS-CATÉGORIE	SCÉNARIOS D'ILLUSTRATION À PARTIR DU CATALOGUE MINISTÉRIEL		TYPOLOGIES DU CATALOGUE MINISTÉRIEL
N°13 / CAT.1.2 Terrorisme	**Scénario A**	Destructions matérielles sur un bâtiment militaire de surface en stationnement à la suite d'une collision avec un drone aérien télépiloté par un terroriste.	CAT.1.2 ACT.2.1 MIL.1 MOP.6.2, MOP.7.5 VEC.1.3 CIB.3.2
N°1 / CAT.3.3 Aléa technologique ou industriel	**Scénario B**	Rejets de particules chimiques dangereuses sur la base navale à la suite d'un accident dans une usine classée « Seveso Haut », située à proximité.	CAT.3.3 ACT.5.3 MIL.1 TMA.10.1 CIB.2.1, CIB.3.4
N°5 / CAT.1.6 Crime organisé	**Scénario C**	Recrudescence de vols de matériels par des délinquants dans l'environnement de la base navale à la suite d'un épisode de violences urbaines dans la zone de sécurité prioritaire (ZSP) la plus proche.	CAT.1.6 ACT.3.2 MIL.2 MOP.6.3 VEC.9.3 CIB.3.2

ÉTAPE 4 Je détermine la probabilité et la gravité des scénarios

Déterminer la probabilité et la gravité des scénarios pertinents sélectionnés me permettra de les cartographier sur une matrice des risques. Pour ce travail, je dois utiliser des échelles de cotation de 1 à 5.

La probabilité correspond à la possibilité qu'un scénario se produise.
La gravité d'un scénario correspond à la mesure des conséquences de l'atteinte à la cible.

DÉTERMINER LA PROBABILITÉ DES SCÉNARIOS

À partir de l'analyse du contexte externe de mon organisation (**ÉTAPE 1**), **je détermine la probabilité des scénarios sélectionnés durant l'ÉTAPE 3** pour mon organisation.

La probabilité correspond à une probabilité d'occurrence d'une source de menace ou d'un aléa. Elle est facilement mesurable quand il s'agit de sinistres statistiquement connus. Lorsqu'il s'agit d'une menace provenant d'une intention humaine, il est possible d'évaluer la probabilité en considérant :

- **la crédibilité d'un scénario** à partir des antécédents d'incident sur le site, le secteur d'activité et l'environnement géographique ;
- **la faisabilité d'un scénario** à partir du niveau de technicité et de ressources des auteurs.

Je peux m'appuyer sur l'échelle de cotation de la probabilité ci-dessous. Je peux l'utiliser en évaluant chaque scénario sur un niveau de probabilité de 1 à 5. Chaque niveau est relié à une description qualitative de l'occurrence possible d'un scénario.

ÉCHELLE DE PROBABILITÉ	
NIVEAU	**DESCRIPTION**
P5. Quasi-certain	Probabilité presque certaine ou événement recensé plusieurs fois sur le site.
P4. Très probable	Probabilité forte ou événement s'étant produit plusieurs fois dans des zones d'activité identiques.
P3. Probable	Probabilité plausible que l'événement se produise (pourrait arriver).
P2. Peu probable	Peut intervenir occasionnellement.
P1. Improbable	Probabilité très faible ou événement improbable. Peut intervenir dans des circonstances exceptionnelles.

IDENTIFIER LES IMPACTS POTENTIELS

Avant de déterminer la gravité des scénarios, **je recense les impacts potentiels de chaque scénario sélectionné** pour mon organisation.

Les **impacts** sont les conséquences de la manifestation d'un événement perturbateur sur mon organisation.

Je peux alors classer les valeurs que j'ai identifiées durant l'**ÉTAPE 2**, en fonction de leur criticité pour l'accomplissement des objectifs et pour la survie de mon organisation. Je dois tenir compte :

- du coût d'un retour à une situation normale ;
- des conséquences sur l'activité d'une perte ou d'une compromission de ma valeur.

Lors de l'identification des impacts principaux, je dois considérer la durée d'interruption d'une activité ou d'une mission et la nature des conséquences sur celle-ci.

Il serait contre-productif de multiplier la nature des impacts. Je peux m'appuyer sur un référentiel commun comme celui ci-après afin de lister la nature des impacts d'un scénario.

Impact humain et social

Intégrité physique, dégradation du moral, mouvement social, difficulté de recrutement / fidélisation, etc.

Impact financier et juridique

Perte de trésorerie, contentieux, responsabilité pénale, amendes, rupture de service ou de contrat, etc.

Impact sur l'image

Atteinte à la réputation, perte de confiance et de crédibilité, etc.

Impact opérationnel

Destructions matérielles, perte technologique ou du savoir-faire, interruption de l'activité, dégradation de la performance, désorganisation durable, indisponibilité, etc.

Impact sur l'environnement

Pollution, dégradation des sols, modification de la faune ou de la flore, etc.

DÉTERMINER LA GRAVITÉ DES SCÉNARIOS

Après avoir identifié les impacts potentiels sur mes valeurs, **je détermine la gravité de chacun des scénarios** sélectionnés au cours de l'**ÉTAPE 3**.

Je peux m'appuyer sur l'échelle de cotation de la gravité ci-dessous. Je peux l'utiliser en évaluant chaque scénario sur un niveau de gravité de 1 à 5 pour mon organisation.

ÉCHELLE DE GRAVITÉ	
NIVEAU	**DESCRIPTION**
G5. Critique	**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. Grave	**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. Significative	**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. Peu significative	**Conséquences 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).

ÉTAPE 4

EXEMPLE BASE NAVALE FICTIVE

DÉTERMINER LA PROBABILITÉ DES SCÉNARIOS

À partir de l'analyse du contexte externe de mon organisation (ÉTAPE 1), je peux déterminer la probabilité de chaque scénario sur une échelle de 1 à 5.

SCÉNARIO	PROBABILITÉ
Scénario A	P4
Scénario B	P2
Scénario C	P5

IDENTIFIER LES IMPACTS POTENTIELS

À partir de l'analyse de mon environnement (ÉTAPE 1), j'identifie les impacts potentiels de chaque scénario pour mon organisation afin de m'aider à évaluer leur gravité ensuite.

SCÉNARIOS D'ILLUSTRATION	IMPACTS POTENTIELS
Scénario A	Indisponibilité du navire Destructions matérielles Désorganisation durable de l'activité Coût de réparation du navire Atteinte à l'image du ministère Pollution maritime par l'éjection des fluides du navire
Scénario B	Fonctionnement en mode dégradé Désorganisation des effectifs Dégradation des performances Atteintes humaines possibles Dégradation du moral Contamination des infrastructures Possible ordre d'évacuation de la zone sinistrée
Scénario C	Destructions et pertes matérielles Coût de réparation ou de rachat du matériel perdu ou dérobé Atteinte à l'image du ministère Atteinte au moral

DÉTERMINER LA GRAVITÉ DES SCÉNARIOS

À partir de l'analyse du contexte interne et externe de mon organisation (ÉTAPE 1), je peux déterminer la gravité de chaque scénario pour mes valeurs sur une échelle de 1 à 5.

SCÉNARIO	GRAVITÉ
Scénario A	G4
Scénario B	G3
Scénario C	G1

PAGE DE NOTES

ÉTAPE 5 Je détermine le niveau de criticité du risque brut

Déterminer le niveau de criticité du risque brut me permettra de cartographier et de hiérarchiser les scénarios pertinents sur une matrice des risques.

Le risque brut est le risque identifié pour l'organisation dont l'évaluation de la criticité se fait avant la prise en compte des moyens de maîtrise. Il correspond à un niveau de criticité brut du risque.

NIVEAU DE CRITICITÉ DU RISQUE

Un **niveau de criticité du risque** peut être déterminé pour un scénario. La criticité correspond à un niveau d'importance d'une menace ou d'un aléa.

Le niveau de criticité du risque peut être déterminé pour calculer un risque brut par la combinaison entre la probabilité et **la gravité pondérée au carré**.
En effet, il est possible de favoriser l'un des facteurs « probabilité » ou « gravité » dans la matrice des risques. La gravité est le plus souvent favorisée par rapport à la probabilité qui reste un critère intrinsèquement incertain et moins objectif que la gravité d'une atteinte.

Niveau de criticité = **Probabilité** x **Gravité²**

DÉTERMINER LE NIVEAU DE CRITICITÉ DU RISQUE BRUT

A présent, **je peux déterminer le niveau de criticité du risque brut sur une matrice des risques** comme celle-ci-après. Je dois effectuer cette opération pour chacun des scénarios pertinents que j'ai sélectionné au cours de l'**ÉTAPE 3**.

Au cours de cette étape, je ne considère pas encore :
- les **mesures de sécurité existantes**, susceptibles de réduire ou supprimer les risques, dont la pondération sera effectuée ultérieurement pour déterminer le risque net (**ÉTAPE 7**) ;
- mon **seuil d'acceptation du risque** que je peux définir afin de m'aider à identifier les risques significatifs maitrisés ou confirmés pour mon organisation (**ÉTAPE 8**).

Je répertorie sur la matrice le niveau de probabilité et le niveau de gravité, évalués lors de l'**ÉTAPE 4**.
Une **matrice des risques** est un outil permettant de classer et visualiser des risques.

J'obtiens un niveau de criticité du risque que je peux positionner sur une échelle à 4 niveaux.

MATRICE DES RISQUES

PROBABILITÉ \ GRAVITÉ²	G1	G2	G3	G4	G5
P5	5	20	45	80	125
P4	4	16	36	64	100
P3	3	12	27	48	75
P2	2	8	18	32	50
P1	1	4	9	16	25

NIVEAU DE CRITICITÉ BRUT	
Risque critique	50 à 125
Risque élevé	25 à 49
Risque moyen	12 à 24
Risque faible	1 à 11

ÉTAPE 5

EXEMPLE BASE NAVALE FICTIVE

DÉTERMINER LE NIVEAU DE CRITICITÉ DU RISQUE BRUT

1. Je cartographie le risque brut de chaque scénario considéré sur la matrice des risques suivante. À partir des évaluations réalisées durant l'**ÉTAPE 4**, je place le niveau de probabilité sur l'axe des ordonnées et le niveau de gravité sur l'axe des abscisses.

MATRICE DES RISQUES						
PROBABILITÉ	GRAVITÉ[2]					
		G1	G2	G3	G4	G5
	P5	SCÉNARIO C	20	45	80	125
	P4	4	16	36	SCÉNARIO A	100
	P3	3	12	27	48	75
	P2	2	8	SCÉNARIO B	32	50
	P1	1	4	9	16	25

2. Par lecture graphique, j'obtiens le niveau de criticité du risque brut de chaque scénario considéré.

SCÉNARIO	PROBABILITÉ	GRAVITÉ	NIVEAU DE CRITICITÉ BRUT	
Scénario A	P4	G4	64	Critique
Scénario B	P2	G3	18	Moyen
Scénario C	P5	G1	5	Faible

ÉTAPE 6 J'identifie les vulnérabilités et les mesures existantes

Identifier les vulnérabilités de mon organisation et analyser son environnement me permettra de prendre la décision de traitement du risque la plus adaptée. Ces données me seront utiles pour déterminer le niveau de criticité du risque net durant l'étape suivante.

Une vulnérabilité correspond à une faiblesse connue de mon organisation susceptible d'être exploitée par des menaces ou d'augmenter l'exposition aux risques.

IDENTIFIER LES VULNÉRABILITÉS

Après avoir recensé les valeurs critiques de mon organisation, **je peux identifier les vulnérabilités potentielles** susceptibles d'augmenter mon exposition à une menace ou à un aléa.

La présence d'une vulnérabilité n'entraîne pas de dommage en elle-même, puisque la présence d'une menace pour l'exploiter est nécessaire. Une mesure de traitement mal mise en œuvre, utilisée de manière incorrecte, ou présentant un dysfonctionnement, peut constituer une vulnérabilité.

Je peux m'appuyer sur les catégories suivantes afin d'identifier les vulnérabilités vis-à-vis d'un scénario.

Matériel

Maintenance insuffisante, stock non protégé, faiblesse d'un composant, mauvaise installation, etc.

Logiciel

Failles connues, mots de passe manquants, absence de sauvegarde et de tests, réglages incorrects, etc.

Réseau

Mauvais câblage, connexion ou voies de communication non protégées, etc.

Personnel

Absence de personnel, formation insuffisante, tâches non maîtrisées, travail non surveillé, etc.

Organisme et partenaires

Absence de contrôle et d'audits, absence de PCA/PRA, défaillance d'un fournisseur, réponse inadaptée, etc.

Infrastructure

Absence de protection physique et d'évacuation, exposition à un aléa, etc.

Les mesures de sécurité existantes sont toutes les mesures déjà mises en place ou prévues afin de réduire l'exposition de mon organisation à une menace ou un aléa.

IDENTIFIER LES MESURES DE SÉCURITÉ EXISTANTES

Je peux maintenant réaliser un diagnostic exhaustif des mesures de sécurité existantes visant à réduire les vulnérabilités de mon organisation à l'égard des scénarios pertinents. Je pourrais alors évaluer le niveau de maîtrise des risques de mon organisation afin de déterminer la criticité du risque net.

À ce stade, je peux recenser les mesures de sécurité existantes parmi :

- les **mesures de prévention**, visant à diminuer la probabilité d'une menace ou d'un aléa, au moyen de solutions organisationnelles, techniques et humaines ;
- les **mesures de protection**, visant à intervenir pour faire cesser une atteinte par la mise en fuite du ou des auteurs, par leur appréhension.

Je peux adopter la démarche suivante afin d'identifier les mesures existantes ou prévues :

- effectuer une **revue du corpus documentaire** relatif aux mesures de sécurité et au management de la sûreté ;
- vérifier les **mesures mises en œuvre** avec les personnes responsables ;
- effectuer une **revue sur site** des mesures de sécurité physique, et de protection dans la profondeur ;
- examiner les résultats des **audits internes.**

ÉTAPE 6

EXEMPLE BASE NAVALE FICTIVE

IDENTIFIER LES VULNÉRABILITÉS

J'identifie les vulnérabilités de mon organisation vis-à-vis des scénarios retenus.

SCÉNARIOS D'ILLUSTRATION	VULNÉRABILITÉS
Scénario A	Vétusté des clôtures extérieures assurant la sécurité périmétrique de la base navale.
Scénario B	Absence d'un plan de continuité d'activité (PCA) d'un prestataire de livraison de produits alimentaires.
Scénario C	Panne de plusieurs caméras de vidéosurveillance surveillant un accès secondaire de la base navale.

IDENTIFIER LES MESURES DE SÉCURITÉ EXISTANTES

J'identifie les mesures de sécurité existantes de réduction des vulnérabilités identifiées de mon organisation, à l'égard des scénarios retenus.

SCÉNARIOS D'ILLUSTRATION	MESURES DE SÉCURITÉ DE RÉDUCTION DES VULNÉRABILITÉS
Scénario A	**Mesures de prévention** • Acquisition de fusils d'interception anti-drone en cas d'intrusion aérienne • Installation d'un dispositif de détection des intrusions, avec remontée d'alarme **Mesures de protection** • Gendarmerie maritime sur site pouvant intervenir en cas d'incident • Renforcement de la résistance des matériaux du navire aux chocs
Scénario B	**Mesures de protection** • Définition d'une procédure de réadaptation de l'organisation du travail en cas d'incident (travail à distance, réallocation du personnel, relèves, etc.) au sein du PCA • Acquisition dans les six prochains mois d'un stock d'équipements de protection individuelle face au risque NRBC (masques, combinaisons, gants, etc.)
Scénario C	**Mesures de prévention** • Fermeture mécanique des accès en périphérie de la base navale • Protection juridique de la base navale en zone protégée (ZP) **Mesures de protection** • Gendarmerie maritime sur site pouvant intervenir en cas d'incident

ÉTAPE 7 Je détermine le niveau de criticité du risque net

Je dois pondérer le risque brut en appréciant les mesures de sécurité existantes et les vulnérabilités de mon organisation. Je détermine alors le niveau de criticité du risque net que je devrai considérer lors de ma décision de traitement du risque.

Le risque net est le risque identifié pour l'organisation dont l'évaluation de la criticité se fait après la prise en compte des moyens de maîtrise. Un risque net peut être un risque significatif confirmé ou un risque significatif maîtrisé.

PONDÉRER LE NIVEAU DE CRITICITÉ DU RISQUE BRUT

Je pondère le niveau de criticité du risque brut de chaque scénario en tenant compte des mesures de sécurité de réduction des vulnérabilités que j'ai recensées au cours de l'**ÉTAPE 6**. Pour chaque scénario, je peux évaluer mon dispositif sûreté en utilisant les critères de mesure suivants.

NIVEAU D'ÉVALUATION DES MESURES DE RÉDUCTION DES VULNÉRABILITÉS		CALCUL	
1	**MESURES ABSENTES.** Dispositif sûreté non présent ou inefficacité évidente pour réduire les vulnérabilités identifiées.	1	x Niveau de criticité brut
2	**MESURES PARTIELLES.** Dispositif sûreté incomplet ne restituant qu'une partie du service et des fonctionnalités attendus pour réduire les vulnérabilités identifiées.	0.8	
3	**MESURES DE SUBSTITUTION.** Dispositif sûreté rendant le service attendu mais sans garantie sur la durée pour réduire les vulnérabilités identifiées.	0.6	
4	**MESURES PERFORMANTES.** Dispositif sûreté garantissant une efficacité sur la durée avec optimisation des moyens pour réduire les vulnérabilités identifiées.	0.4	
5	**MESURES EXCELLENTES.** Dispositif sûreté permettant de réduire au maximum les vulnérabilités identifiées.	0.2	

DÉTERMINER LE NIVEAU DE CRITICITÉ DU RISQUE NET

Je détermine le niveau de criticité du risque net en multipliant le niveau de criticité du risque brut par le coefficient du niveau de mesure de mon dispositif sûreté.

Je peux cartographier le niveau de criticité du risque net sur la matrice pour chaque scénario.

MATRICE DES RISQUES

PROBABILITÉ — NOUVELLE COTATION ↓ — GRAVITÉ[2] — NOUVELLE COTATION ←

	G1	G2	G3	G4	G5
P5	5	20	45	80	125
P4	4	16	36	64	100
P3	3	12	27	48	75
P2	2	8	18	32	50
P1	1	4	9	16	25

Niveau de criticité NET	
Risque critique	50 à 125
Risque élevé	25 à 49
Risque moyen	12 à 24
Risque faible	1 à 11

ÉTAPE 7

EXEMPLE BASE NAVALE FICTIVE

PONDÉRER LE NIVEAU DE CRITICITÉ DU RISQUE BRUT

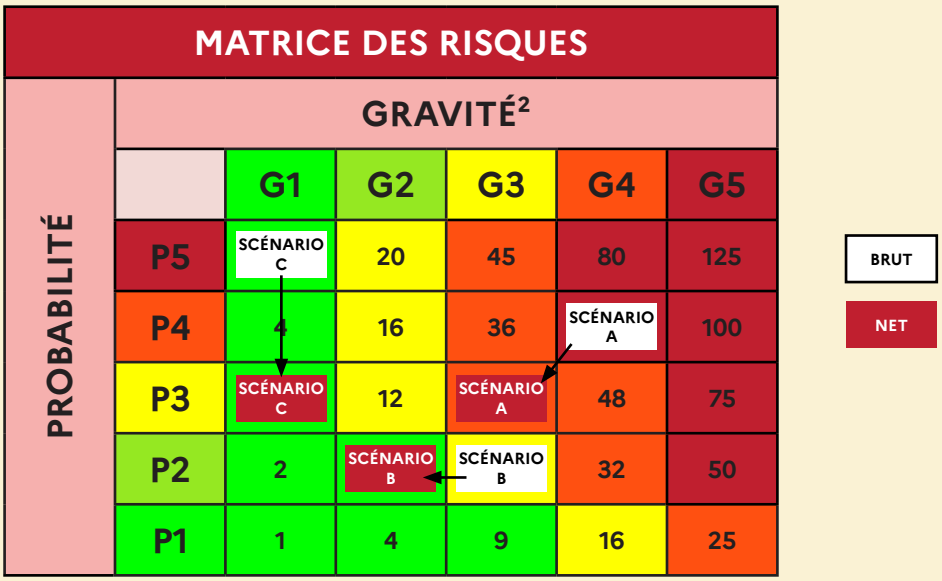
Pour chaque scénario, j'évalue mon dispositif sûreté sur une échelle de niveau de 1 à 5. Puis, je multiplie le niveau de criticité du risque brut par le coefficient du niveau d'évaluation des mesures de réduction des vulnérabilités identifiées.

SCÉNARIOS D'ILLUSTRATION	P	G²	Niveau de criticité BRUT		Évaluation des mesures de réduction des vulnérabilités		CALCUL	NIVEAU DE CRITICITÉ NET	
Scénario A	P4	G4	64	Critique	4	Mesures performantes	64 * 0,4	26	Élevée
Scénario B	P2	G3	18	Moyen	4	Mesures performantes	18 * 0,4	8	Faible
Scénario C	P5	G1	5	Faible	3	Mesures de substitution	5 * 0,6	3	Faible

PONDÉRER LE NIVEAU DE CRITICITÉ DU RISQUE BRUT

Pour chaque scénario, je peux positionner sur la matrice le niveau de criticité du risque net en rouge sur la case correspondante.

J'obtiens l'écart en termes de probabilité et de gravité par rapport au risque brut.



ÉTAPE 8 Je définis mon seuil d'acceptation du risque

Le propriétaire du risque peut déterminer un seuil d'acceptation du risque afin d'identifier les risques significatifs maîtrisés et les risques significatifs confirmés. Ce seuil a pour but d'aider à la prise de décision en matière d'ordre de priorité et de traitement du risque.

Le seuil d'acceptation du risque correspond à la limite en dessous de laquelle les risques identifiés sont considérés comme maîtrisés par le propriétaire du risque, et au-dessus de laquelle ils nécessitent des moyens de maîtrise intégrés à un plan de traitement.

COMMENT DÉTERMINER UN SEUIL D'ACCEPTATION DU RISQUE ?

Afin que le propriétaire du risque établisse un seuil d'acceptation du risque, **j'ai besoin de définir des critères d'acceptation du risque** à partir de l'analyse de l'environnement de mon organisation. Je peux utiliser les données que j'ai recensées lors de l'inventaire réalisé durant l'**ÉTAPE 1** si des critères n'ont pas été définis auparavant par mon organisation durant son processus de management du risque.

DÉTERMINER DES CRITÈRES D'ACCEPTATION DU RISQUE

Les critères d'acceptation du risque sont fixés par le propriétaire du risque et dépendent souvent des politiques, des intentions, des objectifs de l'organisation et des intérêts des parties prenantes.

Il est important que les critères d'acceptation du risque soient élaborés et spécifiés par l'organisation en définissant ses propres échelles d'acceptation des risques. Cette démarche s'inscrit au sein du **processus de management du risque** de mon organisation.

Si des critères ont déjà été définis au sein de mon organisation, le propriétaire du risque peut d'ores et déjà évaluer le seuil d'acceptation du risque de l'organisation et passer à l'étape suivante.

Si des critères d'acceptation n'ont pas encore été définis par mon organisation, le propriétaire du risque peut les déterminer à partir de l'analyse de l'environnement de mon organisation réalisée au cours de l'**ÉTAPE 1**.

Les critères d'acceptation du risque de mon organisation peuvent :

- inclure des seuils multiples, correspondant à un niveau de risque cible souhaité, tout en réservant aux décisionnaires la possibilité d'accepter des risques situés au-dessus de ce niveau dans certaines circonstances définies ;
- être exprimés comme un rapport entre un bénéfice métier (ou un profit estimé) et le risque estimé ;
- correspondre à différents critères s'appliquant à différents types de risques ;
- varier selon la durée d'existence estimée du risque, si celui-ci est par exemple associé à une activité temporaire ou de courte durée.

Afin de **garantir la résilience** de mon organisation, je dois vérifier régulièrement que les critères d'acceptation du risque soient encore valables et cohérents avec le contexte externe et interne de mon organisation. Ce travail doit être effectué durant la phase de surveillance, le contrôle et le réexamen du risque (**ÉTAPE 11**).

Une modification majeure du contexte interne de mon organisation ou une altération du contexte externe dans lequel elle est implantée doit me conduire à réévaluer ces critères.

UTILISER LE SEUIL D'ACCEPTATION DU RISQUE

Le propriétaire du risque peut fixer un **seuil d'acceptation du risque** applicable à mon organisation à partir des critères d'acceptation définis précédemment. Ce seuil peut correspondre aux zones de criticité de mon organisation.

Le seuil d'acceptation du risque est un outil permettant à mon organisation d'identifier :

- les risques significatifs et non significatifs à partir de l'évaluation des risques bruts (**ÉTAPE 5**);
- les risques significatifs confirmés ou maîtrisés à partir de l'évaluation des risques nets (**ÉTAPE 9**), puis traiter les risques significatifs confirmés (**ÉTAPES 10** et **11**).

Les risques significatifs maîtrisés correspondent à ceux qui se situent en-dessous de mon seuil d'acceptation défini par le propriétaire du risque. Ils doivent faire l'objet de mesures de surveillance.

L'**acceptation du risque** est une décision argumentée en faveur de la prise d'un risque particulier. Le seuil aide à déterminer les risques significatifs confirmés et les risques significatifs maîtrisés.

Un seuil d'acceptation du risque d'une organisation peut être illustré de la manière suivante.

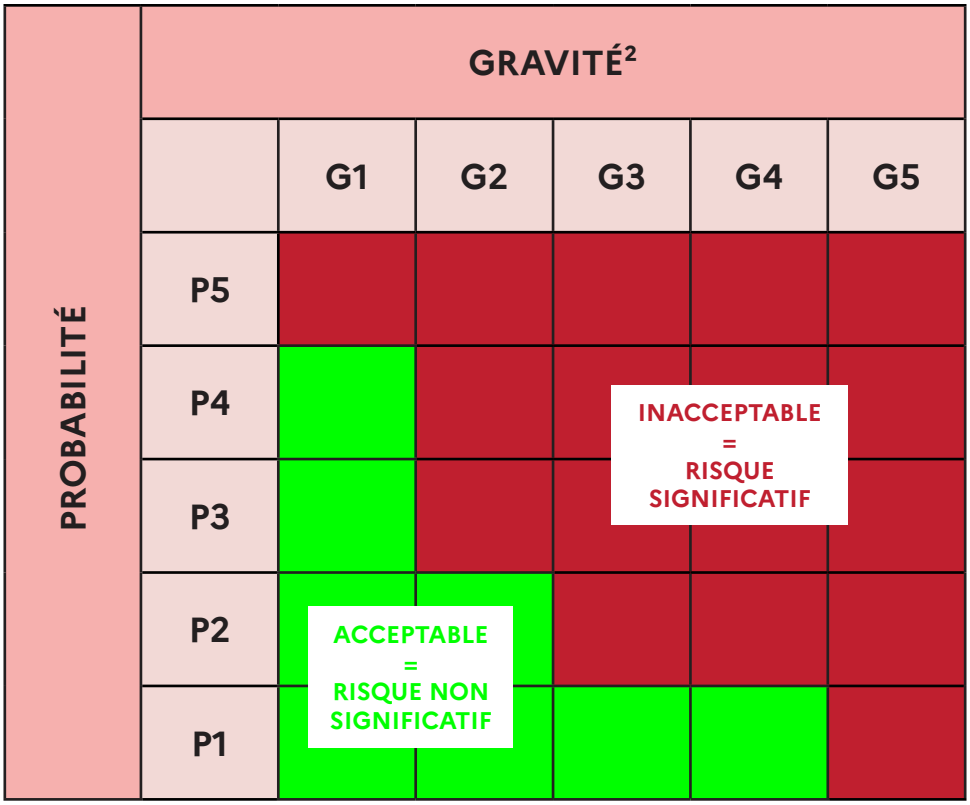


Figure 3. Illustration possible d'un seuil d'acceptation du risque d'une organisation à partir de l'évaluation des RISQUES BRUTS.

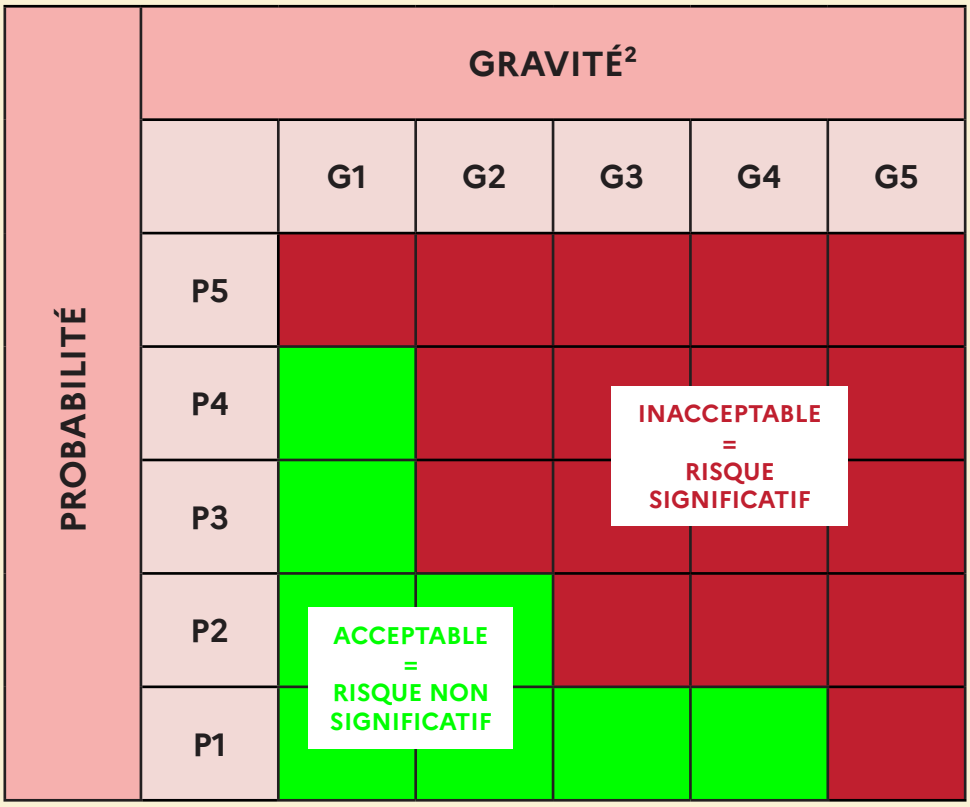
ÉTAPE 8

EXEMPLE BASE NAVALE FICTIVE

DÉTERMINER UN SEUIL D'ACCEPTATION DU RISQUE

Je détermine un seuil d'acceptation du risque, en fonction des critères définis au préalable par le propriétaire du risque.

Avant de coter la criticité du risque net, je fais apparaître le seuil d'acceptation du risque sur la matrice des risques.



PAGE DE NOTES

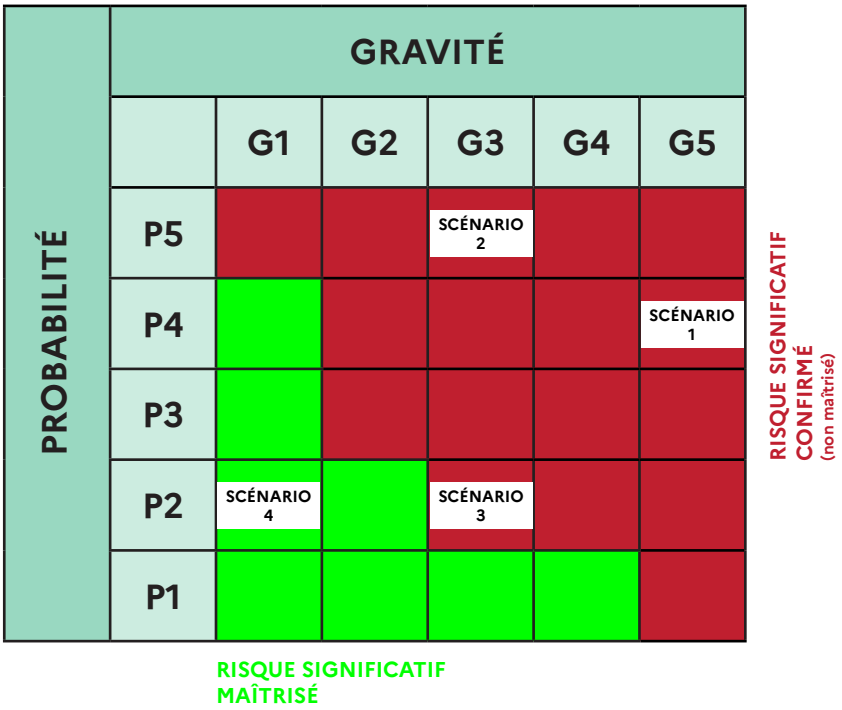
ÉTAPE 9 Je hiérarchise les risques et établis les priorités

Identifier les risques significatifs obtenus lors de l'analyse de risques me permettra de déterminer, parmi eux, les risques confirmés ou maîtrisés. Je peux alors hiérarchiser les risques significatifs et établir des priorités de traitement.

Le risque significatif correspond à un risque dont l'évaluation initiale, lors de la cotation du niveau de criticité du risque brut, est supérieure au seuil d'acceptabilité défini par le propriétaire du risque.

IDENTIFIER LES RISQUES SIGNIFICATIFS

Je peux faire apparaître le seuil d'acceptation du risque, déterminé lors de l'**ÉTAPE 8**, sur la matrice des risques telle que l'illustration ci-après. Je peux positionner chaque scénario sur la matrice obtenue lors de la cotation du niveau de criticité du risque net (**ÉTAPE 7**).



La position de chaque scénario dans la matrice en fonction du seuil d'acceptation du risque permet d'identifier les **risques significatifs maîtrisés** et les **risques significatifs confirmés** (non maîtrisés).
Le seuil d'acceptation permet d'apprécier l'écart entre les moyens existants et les exigences de protection requises en matière de défense et de sécurité.

HIÉRARCHISER LES RISQUES SIGNIFICATIFS

Je peux alors hiérarchiser les risques significatifs sur un tableau selon les deux paramètres suivants :

- Le niveau de criticité du risque net (**ÉTAPE 7**) ;
- Le seuil d'acceptation du risque de mon organisation (**ÉTAPE 8**).

J'obtiens alors une hiérarchisation du niveau de priorité des risques significatifs que je dois considérer lors de l'élaboration du plan de traitement (**ÉTAPE 10**).

SCÉNARIO	CRITICITÉ NET	RISQUE SIGNIFICATIF	PRIORITÉ DE TRAITEMENT
Scénario 1	Critique	Confirmé	1
Scénario 2	Élevé	Confirmé	2
Scénario 3	Moyen	Confirmé	3
Scénario 4	Faible	Maîtrisé	4

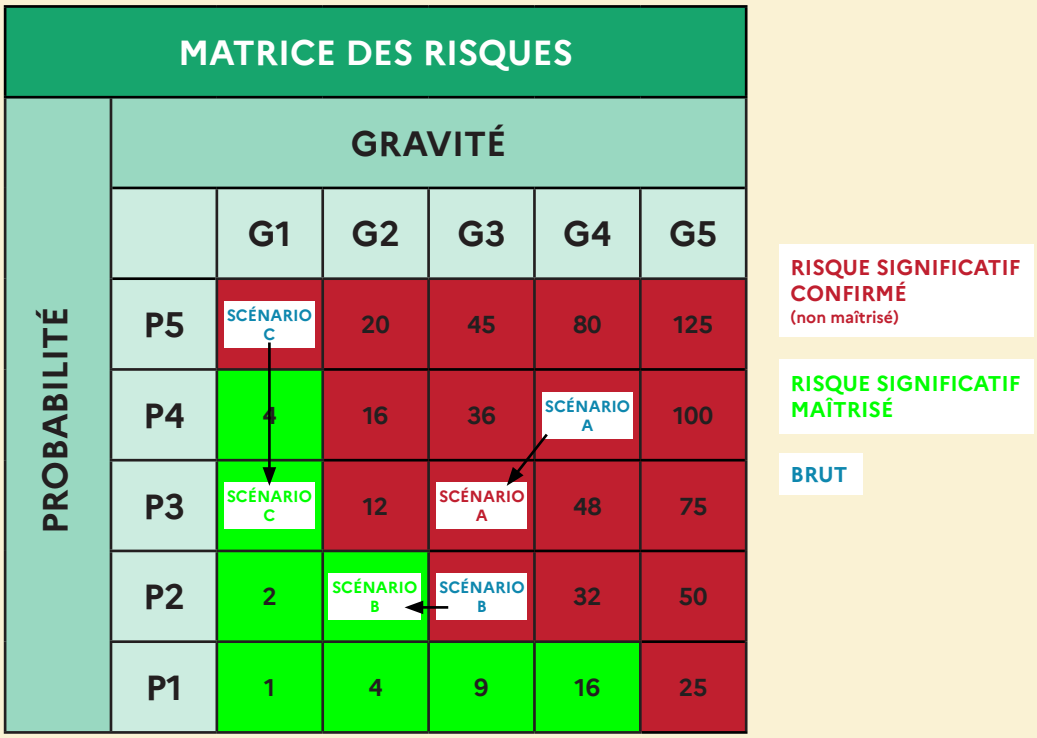
ÉTAPE 9

EXEMPLE BASE NAVALE FICTIVE

IDENTIFIER LES RISQUES SIGNIFICATIFS

Sur la matrice des risques, je positionne à nouveau :
- les risques bruts (en bleu), établis durant l'**ÉTAPE 5** ;
- les risques nets, établis durant l'**ÉTAPE 7** ;
- le seuil d'acceptation du risque de mon organisation, établi durant l'**ÉTAPE 8**.

Parmi les risques nets, j'identifie en fonction de leur position par rapport au seuil d'acceptation :
- les risques significatifs **confirmés** (au-dessus du seuil d'acceptation) ;
- les risques significatifs **maîtrisés** (en-dessous du seuil d'acceptation).



HIÉRARCHISER LES RISQUES SIGNIFICATIFS

Je hiérarchise les risques significatifs pour établir les priorités de traitement.

SCÉNARIOS D'ILLUSTRATION	CRITICITÉ NET	RISQUE SIGNIFICATIF	PRIORITÉ DE TRAITEMENT
Scénario A	26 Élevé	Confirmé	1
Scénario B	Faible	Maîtrisé	2
Scénario C	Faible	Maîtrisé	3

ÉTAPE 10 Je détermine des mesures de traitement

Traiter les risques significatifs a pour objectif de réduire l'exposition de mon organisation aux risques. Je dois déterminer une stratégie de traitement adaptée et établir des mesures de prévention et de protection.

Le traitement du risque est un processus destiné à modifier le risque. Il peut inclure :

- **un refus du risque en décidant de ne pas démarrer ou poursuivre l'activité porteuse du risque ;**
- **la prise ou l'augmentation d'un risque afin de saisir une opportunité ;**
- **l'élimination de la source de risque ;**
- **une modification de la probabilité ;**
- **une modification des conséquences ;**
- **un partage du risque avec une ou plusieurs autres parties incluant des contrats et un financement du risque ;**
- **un maintien du risque fondé sur une décision argumentée.**

DÉFINIR UNE STRATÉGIE DE TRAITEMENT DU RISQUE

Le propriétaire du risque doit désormais définir une stratégie de traitement du risque en choisissant des mesures de sécurité adaptées pour accepter, éliminer ou diminuer les risques.

Plusieurs stratégies de traitement existent pour traiter les risques significatifs identifiés lors de mon analyse (ÉTAPE 9). Ces stratégies ne s'excluent pas mutuellement et peuvent être mises en œuvre simultanément. J'établis une stratégie en définissant des mesures de maîtrise du risque. Elles correspondent à des processus, politiques, actions ou pratiques visant à modifier un risque. Ces stratégies possibles sont illustrées ci-après.

ACCEPTER	ÉLIMINER	DIMINUER
L'**acceptation du risque** consiste à vivre avec le risque et en accepter les conséquences potentielles. Cette stratégie est envisageable pour traiter des **risques significatifs maîtrisés** de faible criticité.	L'**élimination du risque** consiste à éliminer ou refuser une situation d'exposition à un risque. Cette stratégie est envisageable pour traiter des **risques significatifs confirmés** de criticité élevée.	La **diminution d'un risque** consiste à atténuer la probabilité d'un risque ou ses effets. Cette stratégie est appropriée à une diversité de risques et se décline par des **mesures préventives** et **des mesures de protection**.

Le propriétaire du risque applique un plan de traitement. Il met en œuvre les exigences de sécurité adaptées et les mesures opérationnelles selon un **principe d'adaptation** :

- les **mesures permanentes** qui constituent la posture permanente de défense et de sécurité ;
- des **mesures additionnelles**, mises en œuvre de façon circonstanciée et limitée dans le temps, pour faire face à l'aggravation ou à l'évolution de la menace et/ou des vulnérabilités. Elles sont activées notamment en fonction de la posture Vigipirate et des directives interministérielles.

Pour la protection du secret, je dois me référer à :

- **l'instruction générale interministérielle sur la protection du secret de la défense nationale n° 1300/SGDSN/PSE/PSD du 09/08/2021 ;**
- **l'instruction ministérielle n°900/ARM/CAB/NP du 15 mars 2021 relative à la protection du secret et des informations diffusion restreinte et sensibles.**

ÉTABLIR DES MESURES DE PRÉVENTION DU RISQUE

Le propriétaire du risque établit des **mesures de prévention** du risque. Elles correspondent à des dispositifs ou actions propres visant à diminuer la probabilité d'un scénario de menace ou d'un aléa, par combinaison de moyens organisationnels, techniques et humains.

Les mesures de prévention visent à faire obstacle à la réalisation du risque à l'encontre de mes valeurs identifiées durant l'**ÉTAPE 2**, en diminuant en particulier sa probabilité d'occurrence (**ÉTAPE 4**).

Les mesures de renforcement de la protection répondent à une planification préétablie et figurent dans le plan de protection, dans un format adapté à la situation locale. Le dispositif de protection doit être structuré selon les principes de **défense en profondeur** en respectant l'**équation de sûreté**. La défense en profondeur correspond à la superposition de différentes couches de protection, appelées également barrières (périphériques, périmétriques et intérieures).

Les exemples suivants non exhaustifs correspondent à des mesures de prévention.

Actions sur les infrastructures

Protection physique (bloc-porte, chambre forte, garde corps, etc.), protection juridique, surveillance humaine, prévention incendie, dispositifs techniques (détection intrusion, vidéosurveillance, système d'alerte, contrôle d'accès), etc.

Actions sur les systèmes d'information

Politique de sécurité numérique conforme, sauvegardes informatiques, mises à jour régulières, gestion de l'authentification et des données, cloisonnement des réseaux, etc.

Actions sur les fournisseurs

Augmentation des stocks stratégiques sur site, création de circuits de secours, diversification des fournisseurs de la chaîne logistique, obligation de redondance, etc.

Actions sur les ressources humaines

Sensibilisation et mesures comportementales, adaptation contractuelle, exercices de simulation, formation aux risques, etc.

ÉTABLIR DES MESURES DE PROTECTION

Le propriétaire du risque établit des **mesures de protection** qui correspondent à des dispositifs ou actions propres visant à diminuer, réduire ou contenir les effets d'un risque après sa survenue. Les moyens de protection agissent sur la diminution des conséquences du risque, au moyen de solutions organisationnelles, techniques et humaines.

Ces mesures visent à atténuer la gravité (**ÉTAPE 4**) et la portée des conséquences de la survenance d'une menace ou d'un aléa pour mon organisation.

Les exemples suivants non exhaustifs correspondent à des mesures de protection.

Actions sur les infrastructures

Utilisation d'un site alternatif ou d'une capacité de réserve, priorisation de matériels ou de services, relocalisation d'activité, processus alternatifs, etc.

Actions sur les systèmes d'information

Moyens de communication de secours (liaisons satellitaires), restitution des sauvegardes, réinitialisation, fonctionnement dégradé, etc.

Actions sur les fournisseurs

Approvisionnement par un fournisseur alternatif, assistance à un fournisseur critique, etc.

Actions sur les ressources humaines

Travail à distance, réallocation du personnel, recrutement temporaire, réadaptation de l'organisation du travail, dispositif d'intervention ou de réaction armée, etc.

ÉTAPE 11 Je surveille, contrôle et réexamine les risques

Je dois réexaminer le plan de traitement afin de m'assurer que les mesures soient maintenues en condition opérationnelle et adaptées à l'évolution de mon environnement.

La surveillance correspond à la vérification, supervision, observation critique ou détermination de l'état du risque afin d'identifier continûment des changements par rapport au niveau de performance exigé ou attendu. La surveillance peut s'appliquer à un cadre organisationnel de management du risque, un processus de management du risque, un risque ou un moyen de maîtrise du risque.

SURVEILLER ET RÉEXAMINER LES FACTEURS DE RISQUE

Je dois surveiller et réexaminer les risques et leurs facteurs afin d'identifier au plus tôt toute évolution de l'environnement externe et interne de mon organisation (ÉTAPE 1).

Une surveillance constante des menaces est nécessaire afin de détecter tout changement qui pourrait accroître les risques pour mon organisation. Pour cela, je peux m'appuyer sur :

- la réactualisation des Directives nationales de sécurité (DNS) applicables et des instructions ministérielles relatives à la défense et sécurité. Je dois appliquer toute exigence nouvelle liée à une évolution du contexte législatif et réglementaire ;
- une revue des événements et des incidents liés à la sécurité-sûreté de mon organisation.

Je dois aussi tenir compte d'une modification de l'appréciation de mes valeurs et de l'apparition de nouvelles vulnérabilités. En effet, ces évolutions peuvent accroître les risques appréciés auparavant comme des risques de criticité faible.

SURVEILLER, RÉEXAMINER ET AMÉLIORER LE PLAN DE TRAITEMENT

Je dois constamment surveiller, réexaminer et améliorer le processus de gestion des risques afin de garantir que le plan de traitement soit adapté à l'analyse des risques et opérationnel dans la durée.

Je dois m'assurer particulièrement que :

- aucun risque ou élément de risque n'est négligé ou sous-estimé ;
- les actions nécessaires sont mises en œuvre ;
- la compréhension du risque et la capacité à y répondre sont garanties.

Je peux organiser des formations et des entraînements afin de maintenir le plan de traitement en condition opérationnelle.

La **formation** vise à faire acquérir aux personnels les savoir-faire nécessaires pour garantir la protection de mon installation. Ils doivent maîtriser les procédures de sécurité, leurs rôles et leurs responsabilités et les actions à entreprendre en situation de crise et en amont de celle-ci.

Les **exercices** permettent de valider l'opérationnalité du plan de traitement, et de l'améliorer le cas échéant. Ils visent à accroître la réactivité, la coordination et les compétences des parties prenantes de la protection de l'organisation.

Les **retours d'expérience** me permettront d'évaluer l'opérationnalité du plan de traitement et son adéquation avec l'analyse des risques. Je peux aussi m'appuyer sur des indicateurs de performance.

Le plan de traitement s'organise en un **cycle de vie** d'amélioration continue et constitue un processus itératif visant à garantir une efficacité permanente.

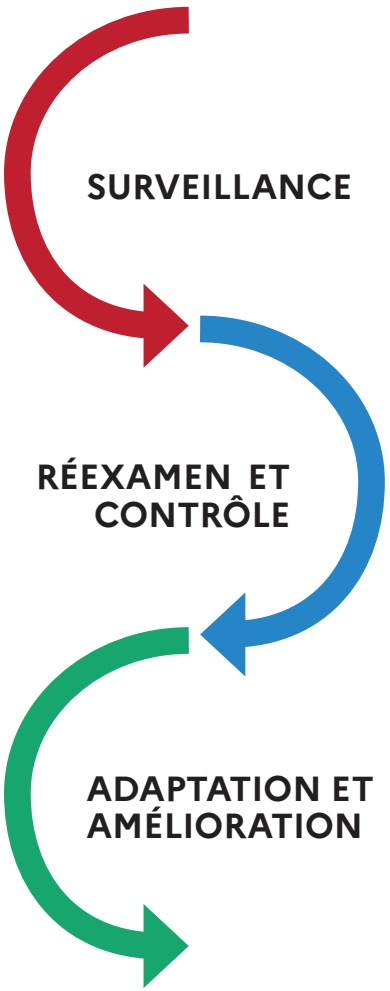


Figure 4. Cycle de vie du plan de traitement.

ANNEXE

SYNTHÈSE DE L'EXEMPLE DE LA BASE NAVALE FICTIVE

SCÉNARIOS D'ILLUSTRATION À PARTIR DU CATALOGUE MINISTÉRIEL		TYPOLOGIES DU CATALOGUE MINISTÉRIEL
Scénario A	Destructions matérielles sur un bâtiment militaire de surface en stationnement à la suite d'une collision avec un drone aérien télépiloté par un terroriste.	CAT.1.2 ACT.2.1 MIL.1 MOP.6.2, MOP.7.5 VEC.1.3 CIB.3.2
Scénario B	Rejets de particules chimiques dangereuses sur la base navale à la suite d'un accident dans une usine classée « Seveso Haut », située à proximité.	CAT.3.3 ACT.5.3 MIL.1 TMA.10.1 CIB.2.1, CIB.3.4
Scénario C	Recrudescence de vols de matériels par des délinquants dans l'environnement de la base navale à la suite d'un épisode de violences urbaines dans la zone de sécurité prioritaire (ZSP) la plus proche.	CAT.1.6 ACT.3.2 MIL.2 MOP.6.3 VEC.9.3 CIB.3.2

SCÉNARIOS D'ILLUSTRATION	P	G^2	NIVEAU DE CRITICITÉ BRUT		RISQUE SIGNIFICATIF / RISQUE NON SIGNIFICATIF ?	COTATION MESURES	NIVEAU DE CRITICITÉ NET	RISQUE MAÎTRISÉ / RISQUE CONFIRMÉ ?
Scénario A	P4	G4	64	Critique	Significatif	4	26	Confirmé
Scénario B	P2	G3	18	Moyen	Significatif	4	8	Maîtrisé
Scénario C	P5	G1	5	Faible	Significatif	3	3	Maîtrisé

SCÉNARIOS D'ILLUSTRATION	PRIORITÉ DE TRAITEMENT
Scénario A	1
Scénario B	2
Scénario C	3

GUIDE PRATIQUE D'ANALYSE DU RISQUE SÛRETÉ DANS LE CADRE DE L'ATAP

à l'usage des organismes du Ministère des Armées et des entreprises de la BITD

Partie 2

INTRODUCTION

L'arrêté du 9 août 2021 portant approbation de l'instruction générale interministérielle n°1300 sur la protection du secret de la défense nationale appelle à la mise en place de mesures de sécurité plus ou moins élevées selon qu'il s'agit de :

- lieux dit « abritant » ;
- ou de lieux, telles que les salles de réunion, où des ISC sont communiqués, échangés ou manipulés mais où ces informations et supports n'ont pas vocation à être conservés.

Dans les deux cas, le système de protection déployé est destiné à protéger les informations et supports classifiés **contre toute menace**, interne ou externe, qui pourrait mettre en cause leur disponibilité, leur intégrité, leur confidentialité et leur traçabilité (DICT) et à empêcher qu'une personne non qualifiée puisse y accéder. **Il s'appuie sur une analyse de risques réalisée par le responsable du site concerné et s'inscrit dans une logique de défense en profondeur** qui repose sur des barrières successives répondant aux critères suivants :

- multifonctions ;
- homogènes ;
- dissuasives ;
- contrôlées ;
- traçables.

La DRSD s'assure de la cohérence de l'analyse de risques et des moyens mis en œuvre pour contrer une atteinte aux informations et supports classifiés, notamment que les mesures de protection physique des locaux et de protection logique des systèmes d'information chargés de la sûreté, qu'elles soient réglementaires ou compensatoires, permettent de détecter une intrusion suffisamment tôt et de la freiner le temps nécessaire à une intervention.
Cette évaluation figure dans l'Avis technique d'aptitude physique (ATAP).

Dans ce contexte réglementaire, il est apparu nécessaire que les organismes de la sphère Défense en charge de réaliser cette appréciation du risque et de mettre en œuvre les mesures de prévention et de protection adéquates disposent d'un socle de connaissances communes et suffisantes pour remplir leur mission. Cette partie concourt à cet objectif.

GÉNÉRALITÉS

TRANSITION D'UNE OBLIGATION DE MOYENS VERS UNE LOGIQUE D'EFFETS À OBTENIR

Avant la refonte de l'IGI 1300 en 2021, la protection du secret de la défense nationale reposait sur une logique de cadre normatif de la protection physique. L'application des prescriptions normatives garantissaient implicitement d'obtenir le résultat attendu. Il s'agissait donc d'une obligation de moyens.

La nouvelle réglementation, si elle ne supprime pas certaines normes de protection physique, impose qu'une analyse didactique de risques soit réalisée pour définir au cas par cas les moyens de prévention et de protection. Il s'agit là d'une logique d'effets à obtenir qui prévaut.

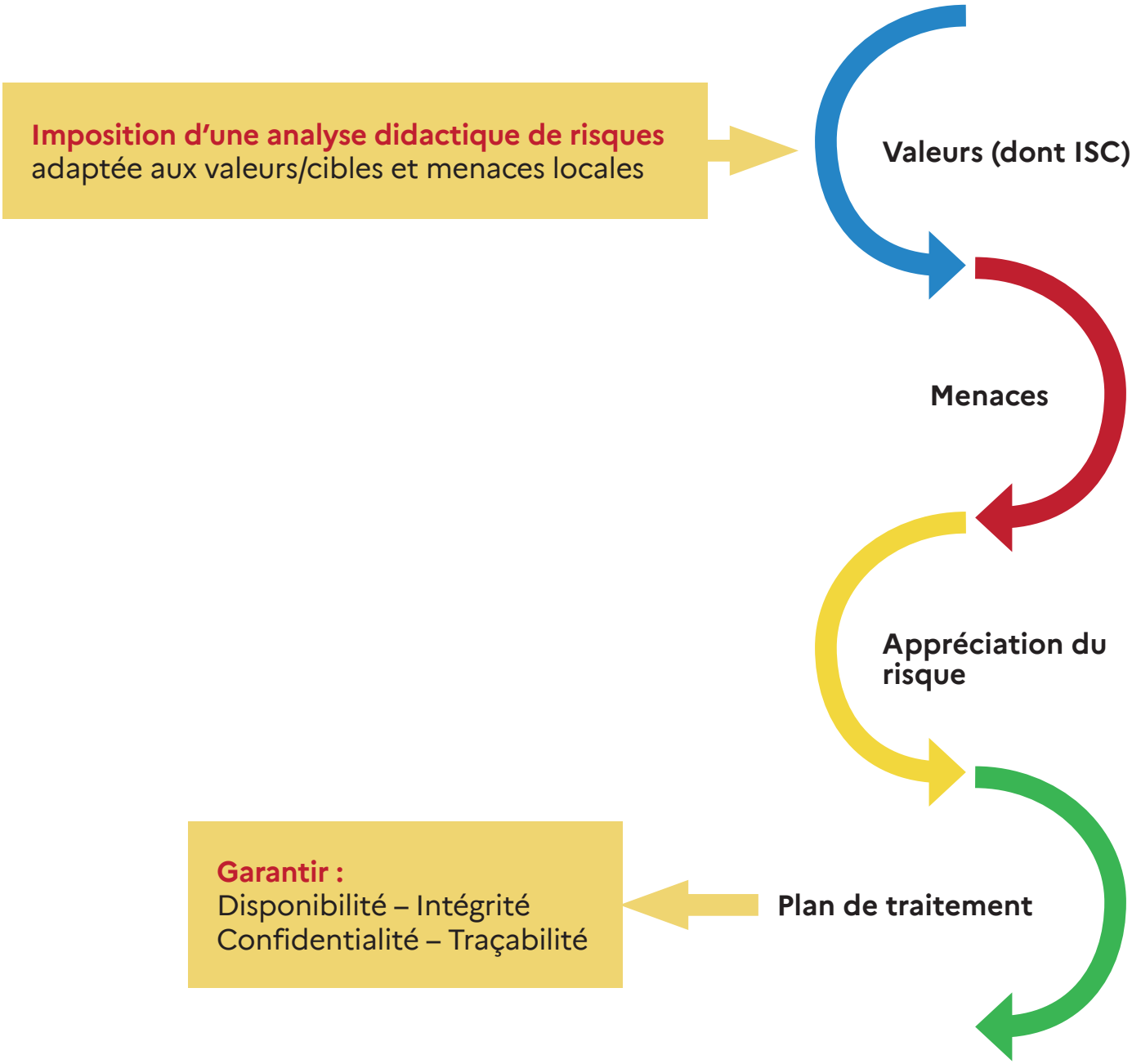


Figure 5. Étapes générales de l'analyse de risques.

CRITÈRES D'ÉVALUATION D'UNE ANALYSE DE RISQUES DANS LE CADRE D'UN ATAP

La DRSD évalue la recevabilité des analyses de risques dans le cadre de la délivrance d'un ATAP pour un local selon des critères définis.
Il est à noter que si l'analyse de risques est certes un élément nécessaire à la constitution du dossier, il n'est pas suffisant.

L'analyse de risques concourt à assurer la protection des informations et supports classifiés dans une logique d'effets à obtenir

Le périmètre de l'analyse de risques sûreté est relatif aux informations et supports classifiés dans le cadre de la délivrance d'un ATAP

L'attendu est donc une démarche intellectuelle didactique et cohérente d'appréciation des risques relatifs aux ISC du lieu concerné par l'ATAP

EN SYNTHÈSE

L'analyse de risques transmise à la DRSD doit permettre d'apprécier si le périmètre (ISC / contexte local) est respecté selon un processus méthodologique d'identification (scénarios), d'analyse (cotation) et d'évaluation des risques par rapport aux mesures identifiées de prévention et de protection dans la profondeur.

1- Respect du périmètre (ISC en tant que valeur / cible et contexte / menaces)
2- Processus méthodologique d'analyse
3- Identification des risques (liste / scénarios)
4- Cartographie des risques (niveau / criticité)
5- Mesures de prévention et de protection dans la profondeur décrites et cotées
6- Évaluation des risques (risques à traiter / risques résiduels)

SOMMAIRE : Une démarche didactique et itérative

La méthodologie consiste à adapter la méthodologie générique d'analyse de risques pour qu'elle réponde aux attendus et critères du dossier de demande d'ATAP. Il est à noter que les étapes 1, 9, 10 et 11 de la première partie sont transposables telles quelles dans le cadre d'une analyse de risques pour un ATAP.

APPRÉCIATION DES VALEURS ET DE L'ENVIRONNEMENT

La **phase d'appréciation des valeurs et de l'environnement** se déroule en deux étapes. Elle correspond à réaliser un inventaire de toutes les données d'entrée de mon organisation nécessaires à la phase d'évaluation du risque.

ÉVALUATION DES RISQUES

La **phase d'évaluation des risques** se déroule en six étapes. Elle correspond à réaliser une cotation et une cartographie du niveau de criticité des scénarios de risques auxquels mon organisation est exposée.

MAÎTRISE ET TRAITEMENT DES RISQUES

La **phase de maîtrise et de traitement des risques** se déroule en deux étapes. Elle correspond à déterminer des mesures de traitement à partir des priorités établies lors de la phase d'évaluation des risques.

SURVEILLANCE, CONTRÔLE ET RÉEXAMEN DES RISQUES

La **phase de surveillance, de contrôle et de réexamen des risques** correspond à une démarche d'amélioration continue des mesures du plan de traitement.

ÉTAPE 1 J'analyse l'environnement de mon organisation

En préliminaire de l'analyse de risques dans le cadre du dossier de demande d'ATAP, je dois collecter toutes les données, informations utiles et nécessaires afin d'appréhender correctement la globalité du contexte, de l'environnement ou de l'écosystème interne et externe de l'organisation.

COMPRENDRE MON ENVIRONNEMENT

Il est essentiel que les informations utilisées pour l'identification des risques soient pertinentes, appropriées et à jour. Il s'agit ici de rentrer davantage dans les particularités de l'organisme étudié pour identifier, en fonction du contexte, de l'environnement local ou général, de la typologie de la menace connue, des cibles répertoriées, les scénarios possibles sur ces cibles et leurs conséquences supposées. Cette étude permet de générer une liste de risques potentiels qu'il faut ensuite analyser. Ces informations sont à fournir par l'organisme au chef de projet ou à l'officier de sécurité en charge de l'analyse du risque sûreté à réaliser pour le dossier d'ATAP.

Cette démarche est identique qu'elle concerne un organisme civil ou militaire.

L'ÉTAPE 1 de la première partie de ce guide est transposable pour la réalisation d'une analyse de risques sûreté dans le cadre d'un dossier de demande d'ATAP.

Tout comme dans la première partie, cette seconde partie déroule un exemple fictif à titre d'illustration.

ÉTAPE 1

EXEMPLE PME FICTIVE, exemple décliné tout au long de cette partie

L'exemple considère une **entreprise de taille moyenne**, SYSCOMDEF, localisée dans une zone industrielle en périphérie d'une grande agglomération. SYSCOMDEF dispose d'un Plan contractuel de sécurité (PCS) actif avec la DGA, est habilitée au niveau de classification secret avec détention et doit réaliser un dossier d'ATAP pour un nouveau local qui sera dédié à abriter des ISC « rangeables » de niveau S relatifs au PCS actif.

ÉTUDIER LE CONTEXTE INTERNE

Les éléments de contextualisation de l'environnement interne recensés ci-dessous sont non exhaustifs et sont proposés à titre d'illustration pour chaque item.

Structure et accessibilité

Configuration du site :
- 1 bâtiment unique composé d'un rez-de-chaussée et d'un étage implanté sur une parcelle d'une superficie de 2 hectares au cœur d'une zone industrielle ;
- 2 accès (1 VHL et 1 piéton) ;
- 1 hall d'accueil, 6 bureaux partagés, 1 bureau d'études, 1 zone de travail sécurisée, 3 ateliers, 2 zones de stockage (dont une sécurisée qui doit faire l'objet d'un ATAP), 2 locaux techniques, 2 salles de réunion ;
- 1 parking à l'intérieur de l'emprise d'une capacité de 48 places VL, 1 quai de chargement /déchargement des marchandises.

Accessibilité : l'accès principal est relié à la route principale qui dessert la ZI. Cet accès est emprunté par le personnel de l'entreprise, les prestataires occasionnels, livreurs et visiteurs.

Utilités et fluides : gaz (réservoirs, réseau de gaz naturel), eau, électricité, ventilation, compresseurs, chauffage, déchets industriels, etc.

Organisation

Organisation fonctionnelle générale :
- 1 président, 1 DG, 1 DRH, 1 DAF, 5 directeurs de SBU, 1 directeur R&D, ...

Répartition des effectifs :
- 114 effectifs permanents ;
- 1 stagiaire, 5 alternants ;
- 6 sociétés prestataires.

Activités

Activités « défense » :
- 1 PCS actif avec détention d'ISC de niveau S ;
- autorité contractante : DGA ;
- part « défense » du CA : 34%.

Activités « hors défense » :
- CA global 3,5 millions € ;
- export dans 26 pays.

Systèmes d'information :
- internet, SI entreprise, 1 SI DR homologué, 1 SI classifié isolé niveau S ;
- applications métiers, etc.

Culture, ouverture :
- partenariats avec des établissements d'enseignement pour le recrutement, participation à des événements (salons, expo, en France et à l'étranger).

Sûreté et sécurité

Lien avec l'ÉTAPE 7.

ÉTUDIER LE CONTEXTE EXTERNE

Politique

Le pays d'implantation de la société est caractérisé par :

- une démocratie libérale et des institutions stables ;
- un temps de paix sur le territoire national, une instabilité géopolitique (conflits internationaux).

Économique

Le territoire d'implantation de la société se caractérise par :

- un niveau de revenus et taux de chômage moyens, une baisse de la démographie ;
- un tissu économique local impacté par la crise COVID 19 qui s'est caractérisée par la fermeture de 21 entreprises dans l'agglomération ;
- des difficultés d'approvisionnement de composants et des matières premières (allongement des délais, ruptures partielles, faillite de fournisseurs).

Social

Le territoire d'implantation de la société se caractérise par :

- un activisme radical régional avec des actions ponctuelles (blocages, manifestations, déprédations modérées) et conflits sociaux (manifestations syndicales en recrudescence) ;
- une présence au sein du territoire : expatriés chinois et russes, étudiants étrangers spécialisés en ingénierie et en intelligence artificielle.

Malveillances

Le contexte de sécurité intérieure de la société est :

- un commissariat de la police nationale localisé à 5 km de la zone industrielle ;
- aucun attentat recensé depuis 10 ans dans un rayons de 100 km de la société ;
- une Zone de sécurité prioritaire (ZSP) à proximité, délinquance locale modérée, augmentation du nombre d'atteintes aux biens (statistiques 2022).

Relations contractuelles

La société entretient des relations contractuelles avec :

- la DGA ;
- 16 sous-traitants et fournisseurs.

Environnemental

La société est exposée à :

- des incendies estivaux ;
- un niveau de sécheresse fort ;
- un niveau de sismicité modéré.

La société est située à 9 km d'une usine de traitement de déchets industriels classée Seveso seuil haut.

ÉTAPE 2 J'identifie mes valeurs ISC

Dans le cadre d'une analyse de risques transmise au dossier de demande d'ATAP, les ISC doivent impérativement être pris en compte et étudiés en termes d'attractivité et d'impact en cas d'atteinte. L'ÉTAPE 2 de la première partie de ce guide est transposable pour la réalisation d'une analyse de risques sûreté dans le cadre d'un dossier de demande d'ATAP.

ÉTAPE 2

EXEMPLE PME FICTIVE

IDENTIFIER LES VALEURS ET ESTIMER LEUR ATTRACTIVITÉ

A partir de l'analyse du contexte interne de mon organisation (ÉTAPE 1), j'identifie mes ISC en tant que valeur.

***Note** : pour le besoin de l'exemple, les types d'ISC recensés ci-dessous sont proposés à titre d'illustration pour chaque item.*

TYPE DE FLUX	VALEURS / CIBLES
	
INFORMATIONS	Informations classifiées papier
	Informations classifiées orales (réunion)
	Informations classifiées numériques
	Supports numériques nomades classifiés
	SI classifiés
	Serveurs

CRITÈRE DE CARACTÉRISATION	1	2	3	4
ATTRACTIVITÉ DE LA VALEUR	La cible n'est pas attractive	La cible est peu attractive	La cible est attractive et/ ou connue de plusieurs personnes	La cible est très attractive et/ ou connue de nombreuses personnes

PAGE DE NOTES

ÉTAPE 3 J'étudie la menace

En fonction du contexte dans lequel ils évoluent, les acteurs de menaces sont plus ou moins présents. Ils se distinguent par les ressources et leurs motivations. Ces critères vont influer sur les scénarios et les modes opératoires. Il est indispensable de prendre en considération la menace externe et la menace interne.

TYPE D'ACTEURS	DESCRIPTION
Étatique	États, agences de renseignement. Attaques généralement conduites par des professionnels, respectant un calendrier et un mode opératoire prédéfinis. Ce profil d'attaquant se caractérise par sa capacité à réaliser une opération offensive sur un temps long (ressources stables, procédures) et à adapter ses outils et méthodes à la topologie de la cible.
Crime organisé	Mafias, gangs, officines. Vols de données à des fins lucratives ou de fraude.
Terroriste	Etatique et/ou idéologique. Attaques habituellement peu sophistiquées mais menées avec détermination à des fins de déstabilisation et de destruction : vol de données sur la protection physique des sites nucléaires pour des actions ultérieures.
Activiste idéologique	Isolé ou organisés en groupe. Modes opératoires et sophistication des attaques relativement similaires à ceux des terroristes mais motivés par des intentions moins destructrices. Certains acteurs vont mener ces attaques pour véhiculer une idéologie, un message.
Officine spécialisée	Profil de « mercenaire » doté de capacités généralement élevées sur le plan technique avec un objectif lucratif. De tels groupes peuvent s'organiser en officines spécialisées proposant de véritables services de cambriolage.Il n'a pas de motivations particulières autres que le gain financier. Des sociétés concurrentes pourraient faire appel aux services de ce type d'auteurs.
Vengeur	Les motivations de ce profil d'attaquant sont guidées par un esprit de vengeance aigu ou un sentiment d'injustice (exemples : salarié licencié, prestataire, client mécontent, ...). Ce profil d'attaquant se caractérise par sa détermination et sa connaissance interne des systèmes et processus organisationnels. Cela peut le rendre redoutable et lui conférer un pouvoir de nuisance important.
Malveillant pathologique	Les motivations de ce profil d'attaquant sont d'ordre pathologique ou opportuniste et parfois guidées par l'appât du gain (exemples : concurrent déloyal, client malhonnête, escroc, fraudeur).
Acteurs extérieurs	Il peut s'agir d'associations, d'ONG, de groupes de presse, d'agences de communication ou d'influence qui, manipulés ou non par un commanditaire, chercheraient à porter atteinte à l'image de l'organisme, de ses dirigeants dans le but de les fragiliser.

L'évaluation de la dangerosité des auteurs peut se mesurer sous cet angle :

RESSOURCES	MOTIVATION +	MOTIVATION ++	MOTIVATION +++
+++	3	6	9
++	2	4	6
+	1	2	3

Il faut garder à l'esprit que l'objectif d'un malveillant n'est pas toujours la cible visée par la menace. Cette cible peut n'être que le moyen de parvenir à son objectif final.

OBJECTIFS DES ACTEURS	DESCRIPTION
Espionnage	Opération de renseignement (étatique, économique). Les secteurs visés sont très larges, variables en fonction des États et du contexte.
Pré-positionnement stratégique	Cible principalement des informations de recherche de pointe.
Influence	Opération visant à diffuser de fausses informations ou à les altérer, mobiliser les leaders d'opinion sur les réseaux sociaux, détruire des réputations, divulguer des informations confidentielles, dégrader l'image d'une organisation ou d'un État. La finalité est généralement la déstabilisation ou la modification des perceptions.
Entrave au fonctionnement	Opération de sabotage visant par exemple à rendre indisponible une installation physique.
Lucratif	Opération visant un gain financier, de façon directe ou indirecte (revente d'informations classifiées, confidentielles ou sensibles).
Défi, amusement	Opération visant à réaliser un exploit à des fins de reconnaissance, de défi ou de simple amusement. Même si l'objectif est essentiellement ludique et sans volonté apparente de nuire, ce type d'opération peut avoir de lourdes conséquences.

ÉTAPE 3

EXEMPLE PME FICTIVE

ÉVALUATION DE LA DANGEROSITÉ DES SOURCES DE MENACE						
Acteurs	Objectifs	Ressources	Motivation	Activité	Évaluation	Priorité
Étatique	Espionnage	3	2	Élevée	Élevée	P1
Étatique	Pré positionnement stratégique	3	2	Moyenne	Élevée	P1
Étatique	Entrave au fonctionnement	3	3	Élevée	Élevée	P1
Étatique	Influence	3	2	Moyenne	Élevée	P1
Officine spécialisée	Pré positionnement stratégique	2	1	Faible	Faible	P2
Officine spécialisée	Espionnage	2	2	Moyenne	Moyenne	P2
Activiste idéologique	Influence	1	2	Moyenne	Faible	P3
Activiste idéologique	Entrave au fonctionnement	1	2	Moyenne	Moyenne	P2
Vengeur	Lucratif	1	1	Faible	Faible	P3
Vengeur	Entrave au fonctionnement	1	1	Faible	Faible	P3
Crime organisé	Lucratif	2	2	Faible	Moyenne	P3
Crime organisé	Entrave au fonctionnement	2	1	Faible	Moyenne	P3
Terroriste	Influence	2	2	Faible	Moyenne	P3
Terroriste	Entrave au fonctionnement	2	1	Faible	Faible	P3

PAGE DE NOTES

ÉTAPE 3 J'étudie la menace

Il faut garder à l'esprit qu'un malveillant se fixe un objectif qu'il réalise en déroulant un scénario selon un mode opératoire pour atteindre une cible.

Acteur → Objectif → Mode opératoire → Cible

MODE OPÉRATOIRE DU SCÉNARIO	DESCRIPTION
Agression verbale	Action qui consiste à interpeller, sans utilisation de la violence physique, une personne ou un groupe de personnes pour lui exprimer son mécontentement. Elle peut être préméditée, de circonstance ou gratuite.
Agression physique	Action qui consiste à utiliser la violence physique à l'encontre d'une personne ou d'un groupe des personnes pour lui exprimer son mécontentement. Elle peut être préméditée, de circonstance ou gratuite.
Blocus intérieur	Action visant à entraver, voire bloquer une ou des activités à l'intérieur d'un site. Cette action, préméditée ou de circonstance, se caractérise par la volonté de prendre possession d'une partie ou de la totalité d'un site.
Blocus extérieur	Action visant à entraver, voire bloquer une ou des activités à partir de l'extérieur d'un site, d'une installation. Cette action, généralement préméditée, se réalise sans pénétration sur le site en prenant possession et/ou en contrôlant un espace proche.
Destruction - Dégradation	Action visant à détériorer ou détruire des biens matériels et/ou immatériels. Cette action qui est généralement l'expression d'un mécontentement peut être préméditée, de circonstance ou gratuite.
Détournement - Utilisation illicite	Action visant à utiliser à son propre profit ou au profit d'un tiers un bien matériel ou un service à l'insu de son propriétaire.
Appropriation frauduleuse - Vol sans violence	Action qui consiste à prendre possession d'un bien matériel ou immatériel appartenant à autrui sans utilisation de la force, ni par la contrainte. Cette action peut être préméditée ou de circonstance.
Vol avec violence	Action qui consiste à prendre possession d'un bien matériel ou immatériel appartenant à autrui par utilisation de la force, de la violence ou par de la contrainte. Cette action peut être préméditée ou de circonstance.
Sabotage	Action visant à détériorer ou détruire sciemment des biens matériels ou immatériels. Cette action préméditée est généralement l'expression d'un mécontentement.
Manipulation - Chantage	Action visant à faire pression sur une personne ou sur un groupe de personnes dans le but d'obtenir une contrepartie. Cette pression psychologique s'exprime par des menaces de divulgation d'informations, d'agression physique sur la victime du chantage ou sur un tiers, de déprédation ou de sabotage.
Espionnage	Action visant à récupérer des informations à l'insu de son propriétaire sans que celui-ci ne puisse s'en apercevoir ni le remarquer. Cette captation d'informations peut être humaine, physique ou technique.
Atteinte à l'image	Action visant à détériorer l'image et la crédibilité d'une personne, d'une marque ou d'un organisme.
Prise d'otage	Action consistant à retenir avec privation de liberté une personne ou un groupe de personnes dans le but d'obtenir des contreparties. Cette action est généralement préméditée et peut être dans certains cas de circonstance.
Enlèvement	Action consistant à séquestrer avec privation de liberté une personne ou un groupe de personnes dans le but d'obtenir des contreparties.
Terrorisme	Action visant à attaquer un lieu déterminé afin de causer des dégâts matériels sur des installations et/ou faire des victimes dans une population donnée. Cette action préméditée a généralement un fort retentissement et génère une pression sur les autorités, l'opinion publique et les cibles touchées.

ÉTAPE 3

EXEMPLE **PME FICTIVE**

TYPE DE FLUX	VALEURS / CIBLES	SCÉNARIOS DE MENACES														
↔		Agression verbale	Agression physique	Blocus intérieur	Blocus extérieur	Destruction	Utilisation illicite	Vol sans violence	Vol avec violence	Sabotage	Manipulation - Chantage	Espionnage	Atteinte à l'image	Prise d'otage	Enlèvement	Terrorisme
INFORMATIONS	Informations classifiées papier					X		X	X	X	X	X				
	Informations classifiées orales (réunion)					X		X	X	X	X	X				
	Informations classifiées numériques					X		X	X	X	X	X				
	Supports numériques nomades classifiés					X		X	X	X						
	SI classifiés					X		X		X	X	X				
	Serveurs					X		X	X	X		X				
HUMAIN	Gouvernance															
	Salariés															
	Stagiaires															
	Prestataires															
	Fournisseurs															
	Clients															
PRODUITS ET BIEN	Matières premières															
	Matières consommables															
	Produits semi-finis															
	Produits finis															
	Machines															
	Équipements															
LOGISTIQUE / MAINTENANCE	Transports															
	Matériel de maintenance															
	Matériel de sécurité															
DÉCHETS / REBUS	Eaux usées															
	Déchets industriels courants															
	Déchets industriels spéciaux															
	Autres effluents															
FLUIDES / ÉNERGIES	Électricité															
	Gaz															
	Eau															
	Combustibles															
	Fluides divers															

L'identification des scénarios permet ensuite de détailler les modes opératoires des acteurs de la menace. Les modes opératoires dépendent du type d'auteur, de ses capacités/moyens, de ses connaissances et de sa motivation. Le mode opératoire varie en fonction de l'acteur et du type de scénario. Néanmoins, il est possible de le séquencer en phases majeures, puis de le décrire.

ÉTAPE 4 Je décris les risques

Lister tous les risques auxquels sont exposées mes valeurs.

La description des risques doit permettre d'identifier de manière sommaire s'il s'agit d'une menace interne, externe, si l'auteur agit par ruse, en toute impunité, par effraction, de jour, de nuit… Cela doit permettre de séquencer le mode opératoire pour apporter par la suite les réponses efficaces.

ÉTAPE 4

EXEMPLE PME FICTIVE

	VALEURS / CIBLES					
MODES OPÉRATOIRES	**Informations classifiées papier**	**Informations classifiées orales (réunion)**	**Informations classifiées numériques**	**Supports classifiés nomades**	**SI classifiés**	**Serveurs**
Destruction - Dégradation	Destruction volontaire de document(s) classifié(s) de la part d'un détenteur par vengeance ou manipulé par un acteur extérieur à l'organisme.	R2	R3	R4	R5	…
Vol sans violence 1	Vol de document(s) classifié(s) papier par un personnel de l'organisme.	R8	…	…	…	…
Vol sans violence 2	Vol de document(s) classifié(s) papier suite à une intrusion (consentie ou non) par un ou des individu(s) extérieur(s) à l'organisme.	…	… R… …		…	…
Vol avec violence	Vol de document(s) classifié(s) papier suite à une intrusion violente par un ou des individu(s) extérieur(s) à l'organisme.	…	…	…	…	…
Sabotage	Destruction volontaire de document(s) classifié(s) par un salarié ou un acteur extérieur à l'organisme.	…	…	…	…	…
Manipulation - Chantage	Pression et menaces sur un personnel de l'organisme pour divulguer des informations issues de document(s) classifié(s).	…	…	…	…	…
Espionnage	Reproduction ou copie illicite (copie / photo) de document(s) classifié(s) papier par un personnel de l'organisme manipulé par un acteur extérieur à l'organisme.	…	…	…	…	…
…	…	…	…	…	…	…

PAGE DE NOTES

ÉTAPE 5 J'évalue la probabilité et la gravité des risques identifiés

Pour cartographier les risques il est nécessaire d'évaluer leur niveau de criticité. Cette criticité est généralement la combinaison de la probabilité que le risque se matérialise avec la gravité de l'atteinte si ce risque se matérialise. Ce résultat est dit « brut » car il ne prend pas en compte les mesures de prévention, ni de protection existantes dont les effets réducteurs ou suppresseurs viendront pondérer utlérieurement cette primo évaluation.

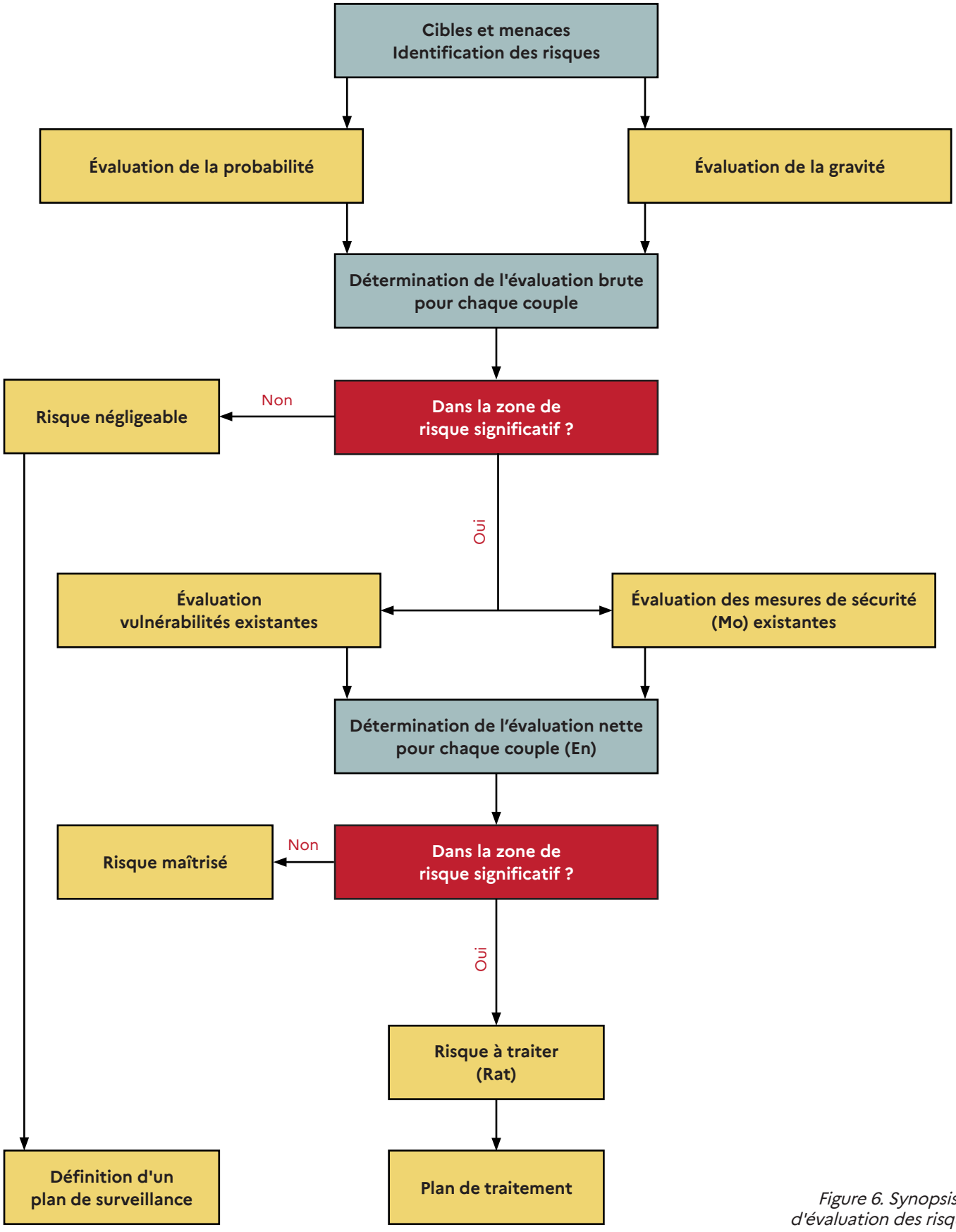


Figure 6. Synopsis d'évaluation des risques.

ÉTAPE 5

EXEMPLE PME FICTIVE

J'évalue la probabilité de survenance du risque.

Si nous reprenons l'échelle de probabilité proposée dans la méthodologie générique de la première partie :

ÉCHELLE DE PROBABILITÉ	
NIVEAU	**DESCRIPTION**
P5 Quasi-certain	Probabilité presque certaine ou événement recensé plusieurs fois sur le site.
P4. Très probable	Probabilité forte ou événement s'étant produit plusieurs fois dans des zones d'activité identiques.
P3. Probable	Probabilité plausible que l'événement se produise (pourrait arriver).
P2. Peu probable	Peut intervenir occasionnellement.
P1. Improbable	Probabilité très faible ou événement improbable. Peut intervenir dans des circonstances exceptionnelles.

N° RÉF.	DESCRIPTION DES RISQUES	PROBABILITÉ
R1-ISCP	Destruction volontaire de document(s) classifié(s) de la part d'un détenteur par vengeance ou manipulé par un acteur extérieur à l'organisme.	Probable 3
R2-ISCP	Vol de document(s) classifié(s) papier par un personnel de l'organisme.	Probable 3
R3-ISCP	Vol de document(s) classifié(s) papier suite à une intrusion (consentie ou non) par un ou des individu(s) extérieur(s) à l'organisme.	Probable 3
R4-ISCP	Vol de document(s) classifié(s) papier suite à une intrusion violente par un ou des individu(s) extérieur(s) à l'organisme.	Peu probable 2
R5-ISCP	Destruction volontaire de document(s) classifié(s) par un salarié ou un acteur extérieur à l'organisme.	Peu probable 2
R...-ISCP	... ...	...

ÉTAPE 6 Je détermine le niveau de criticité brut de chaque risque

J'évalue le niveau de criticité brut des risques pour les cartographier et donc les hiérarchiser par la suite en utilisant la matrice de PROUTY expliquée dans la première partie.

Il est possible de favoriser l'un des facteurs « probabilité » ou « gravité » dans la matrice de PROUTY.

Si par exemple nous manquons de statistiques ou de faits précis pour justifier de la probabilité ou s'il est communément admis que l'importance de l'impact prévaut, alors nous pouvons favoriser le facteur GRAVITÉ.

Le chiffre ou nombre obtenu est le niveau de criticité brut.

MATRICE DES RISQUES						
PROBABILITÉ	GRAVITÉ[2]					
		G1	G2	G3	G4	G5
	P5	5	20	45	80	125
	P4	4	16	36	64	100
	P3	3	12	27	48	75
	P2	2	8	18	32	50
	P1	1	4	9	16	25

Niveau de criticité NET	
Risque critique	50 à 125
Risque élevé	25 à 49
Risque moyen	12 à 24
Risque faible	1 à 11

ÉTAPE 6

EXEMPLE **PME FICTIVE**

DESCRIPTION DES SCÉNARIOS	P	G	CRITICITÉ BRUTE
Destruction volontaire de document(s) classifié(s) de la part d'un détenteur par vengeance ou manipulé par un acteur extérieur à l'organisme.	4	4	64
Vol de document(s) classifié(s) papier par un personnel de l'organisme.	4	5	100
Vol de document(s) classifié(s) papier suite à une intrusion (consentie ou non) par un ou des individu(s) extérieur(s) à l'organisme.	3	4	48
Vol de document(s) classifié(s) papier suite à une intrusion violente par un ou des individu(s) extérieur(s) à l'organisme.	2	5	50
Destruction volontaire de document(s) classifié(s) par un salarié ou un acteur extérieur à l'organisme.	2	4	32
... ...	...	...	...

MATRICE DES RISQUES

PROBABILITÉ	GRAVITÉ[2]				
	G1	G2	G3	G4	G5
P5	5	20	45	80	125
P4	4	16	36	R1-ISCP	R2-ISCP
P3	3	12	27	R3-ISCP	75
P2	2	8	18	R5-ISCP	R4-ISCP
P1	1	4	9	16	25

ÉTAPE 7 J'évalue mon dispositif de sûreté

Il s'agit ici de réaliser un diagnostic exhaustif des mesures de prévention, de protection et de réaction mises en œuvre sur le site dans le but d'évaluer le niveau de maîtrise des risques. Les vulnérabilités identifiées sont également relevées.
Les informations collectées au cours de l'étape d'étude de l'environnement de l'organisme seront notamment exploitées à cette fin.

FACTEUR D'AMBIANCE

- culture sûreté
- application des principes de sûreté
- sensibilisation du personnel
- climat social
- environnement extérieur
- prévention situationnelle
- failles, vulnérabilités
- ...

MESURES ORGANISATIONNELLES

- organisation, fonctionnement, positionnement de la structure de sécurité
- corpus doctrinal du management de la sûreté (politique de sûreté, procédures, fiches réflexes, plans de gestion de crise, PCA, PRA, règlement intérieur, charte informatique, ...)
- gestion des flux
- zonage du site
- contrats de maintenance
- dispositifs de contrôle
- exercices
- ...

INFRASTRUCTURE ET MOYENS TECHNIQUES

- protection mécanique dans la profondeur et barrières successives
- protection des accès
- détection intrusion
- contrôle d'accès
- vidéosurveillance
- dispositifs d'alarme et d'alerte
- vétusté et obsolescence des moyens et technologies
- résistance des matériaux
- ...

RESSOURCES HUMAINES

- effectifs dédiés à la sûreté
- compétence du personnel
- formation du personnel
- entraînement du personnel
- relation avec les forces de sécurité intérieure
- relation avec l'inspecteur référent de la DRSD

Chaque mesure ou vulnérabilité doit être évaluée et rapportée à chaque risque pour déterminer son effet pondérateur ou aggravant.

ÉTAPE 7

EXEMPLE PME FICTIVE

Pour évaluer les mesures et dispositifs existants et de déceler les vulnérabilités de ma société, j'utilise cinq niveaux de critères :

Niveau 1	Mesure ou moyen **ABSENT** = Système de protection non présent ou inefficacité évidente	**Niveau critique**
Niveau 2	Mesure ou moyen **PARTIEL** = Système de protection incomplet ne restituant qu'une partie des résultats attendus	**Niveau insuffisant**
Niveau 3	Mesure ou moyen DE **SUBSTITUTION** = Système présent qui rend le service attendu mais sans garantie sur la durée	**Niveau fragile**
Niveau 4	Mesure ou moyen **PERFORMANT** = Système qui garantit l'efficacité dans le temps avec optimisation des moyens	**Niveau efficace**
Niveau 5	Mesure ou moyen **EXCELLENT** = Système qui fait référence dans ce domaine	**Niveau très satisfaisant**

La société SYSCOMDEF a réalisé un autodiagnostic interne dans 5 domaines :

- organisationnel et corpus documentaire du management de la sûreté
- sûreté des personnes, sensibilisations et habilitations
- sécurité des ISC
- sécurité physique du site
- sécurité des SI

ÉTAPE 7

EXEMPLE PME FICTIVE

Les grilles ci-dessous sont indicatives et peuvent être complétées suivant le cas étudié.

DOMAINE ORGANISATION DE LA PROTECTION		
SYSCOMDEF		**Note**
1 - STRUCTURE DE SECURITÉ		**3,89**
1	L'entité dispose d'une structure de sécurité	4
2	L'organisation et les missions sont décrites dans un document cadre	4
3	L'effectif alloué aux missions relatives à la sécurité est suffisant	4
4	La charge de travail et le temps consacrés aux missions de sécurité sont suffisants	4
5	Le personnel chargé de la sécurité a reçu une formation spécifique à la sûreté	4
6	L'OSE dispose-t-il d'un document de désignation signé par le représentant légal ?	3
7	Le personnel de la structure de sécurité dispose d'un agrément	4
8	L'organisme dispose d'un BPS car il détient des ISC de niveau TS	4
9	Le personnel est habilité au bon niveau	4
2 - GESTION DES RISQUES		**3,25**
10	Il existe un document déclinant la politique de sécurité globale	2
11	Il existe une analyse globale des risques sur les activités	3
12	L'entité dispose d'une organisation (humaine) de prise en compte des risques	3
13	L'entité dispose d'un document cadre fixant les directives et orientations de l'analyse et du traitement de ses risques	3
14	L'entité dispose de moyens dédiés à la gestion des risques	3
15	L'analyse des risques relatifs aux ISC est réalisée	3
16	L'entité n'a pas externalisé tout ou partie de son processus de management des risques relatifs aux ISC	3
17	L'entité a listé et priorisé ses valeurs ou cibles potentielles d'atteintes	4
18	L'analyse des risques dans le cadre d'un ATAP répond aux critères de reçevabilité de la DRSD	3
19	L'entité a identifié et listé tous les risques potentiels auxquels elle peut être confrontée	4
20	L'entité a décrit et mesuré l'efficacité de ses mesures de prévention et de protection dans la profondeur	4
21	L'entité a évalué des risques à traiter	4
3 - PLANS DE CONTINUITÉ / REPRISE D'ACTIVITÉ (PCA / PRA)		**2,00**
22	L'entité a formalisé des PCA et PRA relatifs aux risques identifiés	2
23	Les domaines impactant les PCS sont couverts	2
4 - TRAITEMENT DES INCIDENTS		**3,00**
24	Il existe une procédure de traitement des incidents	3
25	Il existe un outil de remontée d'informations	3
26	L'entité exploite les incidents régulièrement à des fins de retour d'expérience et d'évolution des moyens de maîtrise des risques	3
5 - GESTION DE CRISE (GDC)		**1,00**
27	L'entité dispose d'une organisation et de procédures de GDC	1
28	L'entité dispose d'un plan de formation en GDC	1
29	L'entité conduit des exercices de GDC	1
TOTAL		**2,63**

ÉTAPE 7

EXEMPLE **PME FICTIVE**

DOMAINE SÉCURITÉ DES PERSONNES		
SYSCOMDEF		**Note**
1 - CIRCUIT ARRIVÉ ET DÉPART		**3,88**
1	Il existe une procédure formalisée et communiquée décrivant le circuit d'arrivée des nouveaux collaborateurs	4
2	Si, oui : Le circuit d'arrivée est composé d'une sensibilisation par la chaîne de sécurité	4
3	Le circuit d'arrivée est composé d'une démarche sécurisée de délivrance des droits d'accès, badge et clefs	4
4	Le circuit d'arrivée est composé de la signature d'un engagement de responsabilité pour les personnes habilitées (si concerné)	4
5	Il existe une procédure formalisée et communiquée décrivant le circuit de départ	4
6	Le circuit de départ est composé de la signature de l'engagement de responsabilité pour les personnes habilitées	4
7	Le circuit de départ est composé de la remise et désactivation du badge et autre matériel (clefs, SIC)	4
8	Le circuit départ est composé de la suppression de tous les droits informatiques et adresses de messagerie électronique ainsi que de la restitution des différents matériels informatiques et de communication (ordinateur, ordiphone, périphérique de stockage externe, etc.)	3
2 - GESTION DES HABILITATIONS		**3,25**
9	Il existe une procédure formalisée et appliquée décrivant la gestion des habilitations	4
10	La gestion, même non formalisée, comprend l'alimentation des pièces dans un dossier personnel comprenant la notice individuelle, la signature du 1er volet de l'engagement de responsabilité, la décision d'habilitation	4
11	La gestion, même non formalisée, comprend une sensibilisation annuelle	2
12	La gestion, même non formalisée, comprend le respect du besoin d'en connaître par les chargés de projet	3
13	La gestion, même non formalisée, comprend un suivi de la durée de validité de l'habilitation	3
14	Le registre ou l'application de gestion des habilitations est de niveau DR ou Confidentiel personnel	2
15	Le niveau de protection des dossiers papiers est suffisant	4
16	Les dossiers (numérisés ou papiers) sont conservés plus d'un an après échéance de l'avis de sécurité	4
3 - GESTION DES STAGIAIRES, APPRENTIS, ALTERNANTS		**4,00**
17	Ces catégories de personnel n'ont pas accès aux ISC ou bien les procédures sont strictement identiques au personnel permanent de l'organisme	4
18	La chaîne de sécurité participe à la gestion des stagiaires	4
19	La société applique une procédure liée à la sûreté dans la gestion des stagiaires	4
20	Cette catégorie de personnel est sensibilisée à son arrivée	4
21	Il existe une clause de confidentialité dans le contrat du stagiaire	4
22	La chaine Sécurité est associée à la relecture des mémoires et productions des stagiaires/ apprentis/alternants/doctorants	4
4 - POLITIQUE DE SENSIBILISATION		**2,86**
23	Il existe une politique de sensibilisation du personnel	3
24	La politique de sensibilisation du personnel comprend les actions spécifiques au volet de la PSDN	3
25	Ces sensibilisations sont tracées	2
26	La fréquence des séances de sensibilisation est définie, régulière et adaptée aux besoins	3
27	Les personnes habilitées sont sensibilisées annuellement	3
28	Le personnel est sensibilisé à la sécurité des systèmes d'information	3
29	Le personnel partant à l'étranger reçoit une sensibilisation spécifique	3
TOTAL		**3,50**

ÉTAPE 7

EXEMPLE **PME FICTIVE**

DOMAINE SÉCURITÉ DES ISC		
SYSCOMDEF		**Note**
1 - PRINCIPES GÉNÉRAUX DE CLASSIFICATION		**3,14**
1	Les règles de marques des matériels et ISC sont conformes à la réglementation quel que soit le niveau de classification	4
2	L'enregistrement des ISC TS est réalisé par le BPS	4
3	L'enregistrement est réalisé par l'intermédiaire d'un système respectant les rubriques du modèle présenté dans l'IGI1300	4
4	L'enregistrement permet d'attribuer sans ambiguïté l'attribution à un détenteur	4
5	Les ISC sont enregistrés dans l'ordre chronologique	4
6	L'échéance de classification est indiquée	1
7	Un dispositif permet de suivre les mouvements des ISC (Fiche de position par exemple)	1
2 - GESTION DES ISC		**4,00**
8	Le BPS est responsable de la conservation des ISC	4
9	Des meubles de sécurité approuvés sont utilisés pour les ISC rangeables	4
10	Une procédure existe et est appliquée concernant l'utilisation et la conservation des ISC non rangeables	4
11	Les clés des lieux abritant sont conservées de manière sécurisée sur le site	4
12	Les informations classifiées dématérialisées sont stockées sur un système d'information homologué au même niveau de classification	4
13	Les procédures relatives aux changements de combinaison sont conformes avec la réglementation	4
14	La copie de la combinaison est conservée sous enveloppe opaque fermée et dans un meuble de sécurité	3
15	La conservation des ISC permet d'assurer le besoin d'en connaître (cloisonnement par projet. Sous-coffre)	5
16	L'exploitation des ISC Très Secret est toujours réalisée en zone réservée	4
17	L'accès aux lieux abritant des ISC à des personnes n'ayant pas le besoin d'en connaître est cadré (contrat sensible)	4
18	L'inventaire annuel est réalisé par les détenteurs sous la supervision de l'OS ou bureau de protection du Secret	4
19	Un procès-verbal (PV) est réalisé à chaque inventaire. Il mentionne les références et l'identification de chaque support classifié	4
3 - RÉCEPTION DIFFUSION ACHEMINEMENT DES ISC		**3,75**
20	Le BPS ou l'OS sont responsables de la réception et de l'expédition	4
21	L'intégrité de l'emballage est vérifié	4
22	Le destinataire procède à son enregistrement dès réception	4
23	La reproduction des ISC est systématiquement tracée ?	3
24	Pour le TS la reproduction totale ou partielle est effectuée après autorisation écrite de l'autorité émettrice et l'organisme dispose d'écrits justifiant de cette autorisation dans le cas de reproduction réalisée	4
25	Il existe des procédures et des moyens d'évacuation et de destruction d'urgence des ISC	3
26	La destruction des ISC est encadrée selon leur niveau de classification et il existe des PV	4
27	Les mesures prises pour le transport en dehors d'une zone protégée sont conformes à la réglementation	4
TOTAL		**3,63**

ÉTAPE 7

EXEMPLE **PME FICTIVE**

DOMAINE SÉCURITÉ PHYSIQUE DU SITE (EXTRAIT)		
SYSCOMDEF		**Note**
1 - PROTECTION DE L'EMPRISE		**3,29**
1	L'emprise est clairement délimitée	4
2	Le site est ceint d'une clôture solide ou végétale qui n'est pas franchissable sans facilitateur de franchissement	5
3	Il existe un système de détection d'intrusion couvrant les parties extérieures de l'emprise	1
4	L'emprise est érigée en ZONE PROTEGÉE	4
5	Les parties extérieures disposent d'un éclairage uniforme et global qui n'offre pas de zone d'ombre	4
6	Les accès en périphérie sont verrouillés mécaniquement en HNO	1
7	Des contrôles de conformité sont faits régulièrement par la structure de sûreté	4
2 - SÉCURITÉ DES BÂTIMENTS		**3,67**
8	Le(s) bâtiment(s) ne présente(nt) pas de parties de parois de faible résistance (PPFR)	3
9	Le ou les bâtiment(s) ne comporte(nt) pas de points d'accès singuliers (circulations verticales horizontales conduits d'arrivée évacuation d'eau, conduits techniques, etc.) qui pourraient faciliter l'accès aux locaux	4
10	Il existe un système de détection d'intrusion sur les bâtiments	4
3 - CONTRÔLE DES ACCÈS (CA)		**3,78**
11	Le site dispose d'un dispositif d'accueil et de filtrage des accès, qu'il soit organisationnel, technique ou humain	4
12	Les accès en périmètrie (Bloc-Portes battant-coulissants, TQ en produit verrier) sont vérouillables et verrouillés mécaniquement	3
13	Les ouvrants en périmètrie (châssis vitré avec produit verrier) sont fixes/battants dotés de dispositifs de protection (barreaux/châssis renforcé avec produit verrier antieffraction)	4
14	Une personne ne peut pas pénétrer sur le site sans avoir été au préalable identifiée et autorisée	3
15	La faiblesse potentielle des ouvrants périmétriques est rattrapée par des dispositifs physiques adaptés	5
16	Il existe une politique de gestion des accès	4
17	La gestion des prestataires est encadrée par une procédure	4
18	Les prestations font l'objet d'un plan de prévention/protocole de sécurité incluant des mesures de sûreté (port d'une tenue, badges particuliers, exclusion de zones horaires particuliers)	4
19	Il existe un dispositif visuel d'identification des types d'accédants (permanent, prestataire permanent, prestataire occasionnel, stagiaire, etc.)	4
20	La gestion des visiteurs fait l'objet d'une procédure ad hoc et elle est appliquée	4
21	Un dispositif permet d'annoncer au préalable un visiteur	4
22	L'identité de chaque visiteur est contrôlée	4
23	La décision d'autoriser une visite est confiée à la structure de sûreté pour les zones désignées comme sensibles (locaux abritant, zones de valeurs de l'organisme)	3
24	Les visiteurs sont accompagnés en permanence sur le site	4
25	Le mode escorte du CA est activé	3
26	Une personne désignée comme représentant le chef d'organisme est en mesure de refuser l'entrée d'un visiteur	4
27	La tentative de modification des droits génère une alerte notamment pour les lieux sensibles (lieux abritant et lieux contribuant à la sécurité de ces derniers)	4
28	Le bâtiment dans lequel se trouve les locaux abritant est placé sous contrôle d'accès	4
29	La gestion et l'affectation des droits dans le système de contrôle d'accès électronique est gérée par la structure de sûreté	4
32	Le local alimentant et hébergeant le système de CA est sécurisé	4
33	Le système de contrôle d'accès est homologué	4
34	Le CA a fait l'objet d'une évaluation CYBER lors de la visite de site par un tiers ou par la société	4
35	La neutralisation d'un badge perdu ou volé est réalisée sans délai	3
37	La fonction anti pass back est mise en œuvre	1
6 - SYSTÈME DE DÉTECTION INTRUSION ET D'ALARME (DI)		**3,00**
56	Un système de DI existe et est fonctionnel	4
57	Des tests sont réalisés régulièrement et ont donné lieu à une détection effective et une levée de doute effectuée dans des délais acceptables	4
58	La fiabilité cyber du système a été évaluée	1
62	Le site a fait l'objet d'une reconnaissance des FSI en cas de nécessité d'intervention	1
8 - LOCAUX ABRITANT LES ISC		**4,00**
63	Le ou les locaux ne présente(nt) pas de vulnérabilités physiques voire logiques contraires aux exigences de la réglementation	4
64	Les clés des locaux abritant restent sur le site et sont sécurisées (armoire à clé combinaison mécanique ou armoire à clé liée au CA)	4
TOTAL		**3,39**

ÉTAPE 7

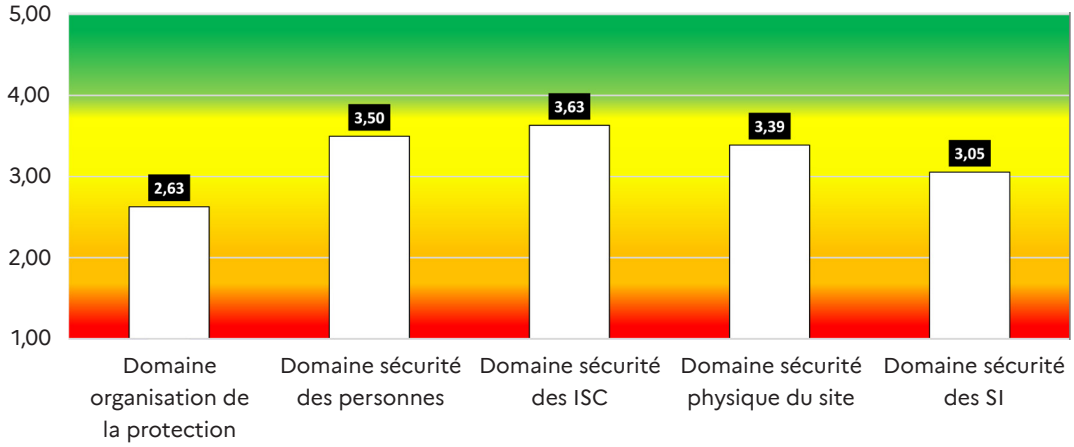
EXEMPLE **PME FICTIVE**

DOMAINE SÉCURITÉ DES SI		
SYSCOMDEF		**Note**
1 - POLITIQUE DES SI		**3,00**
1	Il existe une Politique de Sécurité des Systèmes d'Information (PSSI)	3
2	La PSSI est récente (- 3 ans)	3
4	Cette PSSI est une déclinaison de la PSSI du groupe	3
2 - GOUVERNANCE DE LA SSI		**3,00**
5	La fonction de RSSI existe	3
6	la fonction de RSSI est exercée en interne	3
7	Sa fonction est clairement identifiée au sein de l'entité	3
8	Le RSSI fait partie intégrante du service informatique de l'entité	3
9	Le RSSI occupe de 80 à 100% de son de temps à la fonction	3
10	Le RSSI dispose d'un suppléant	3
11	Le RSSI est informé des incidents	3
3 - MAINTIEN EN CONDITION DES SI		**3,00**
12	Le service informatique est externalisé	3
13	Le MCS (maintien en condition de sécurité) ou le MCO (maintien en condition opérationnelle) n'est pas externalisé	3
14	Le contrôle de la maintenance est réalisé en continue	3
4 - PROTECTION JURIDIQUE DES SI		**4,00**
15	Il existe une charte informatique émargée par les salariés	5
16	Il existe une charte informatique spécifique destinée au personnel du service informatique	4
17	Il existe une charte informatique destinée aux intervenants extérieurs, stagiaires, apprentis, alternants, doctorants	4
5 - SENSIBILISATION AUX MENACES CYBER		**4,00**
18	L'entité a mis en place une politique de sensibilisation aux menaces cyber	4
19	L'entité a mis en place des séances de sensibilisation aux menaces cyber pour le personnel	4
20	L'entité a mis en place des séances de sensibilisation aux menaces cyber pour les stagiaires, alternants, apprentis	4
6 - TRAITEMENT DES INCIDENTS CYBER		**1,20**
21	Une procédure de constitution de preuves informatiques est prévue en cas de découverte de perte ou de vol de données	2
22	L'accès en écriture des journaux de traçabilité (logs) est autorisé au service informatique	1
23	Il existe une procédure définie et connue de tous en cas d'incident (physique ou logique) sur les SI	1
24	Des exercices de reprise après sinistre sont effectués	1
TOTAL		**3,05**

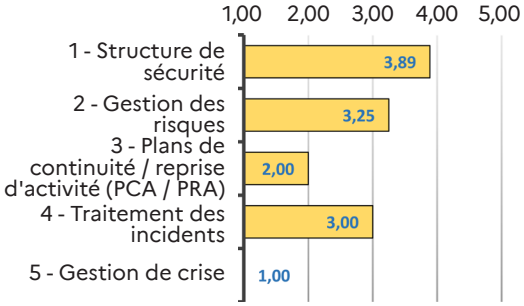
ÉTAPE 7

EXEMPLE **PME FICTIVE**

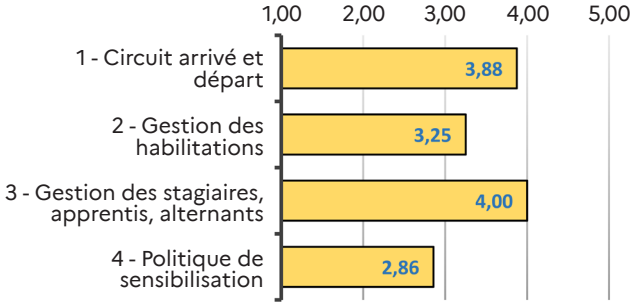
ÉVALUATION DE LA SÛRETÉ PAR DOMAINE



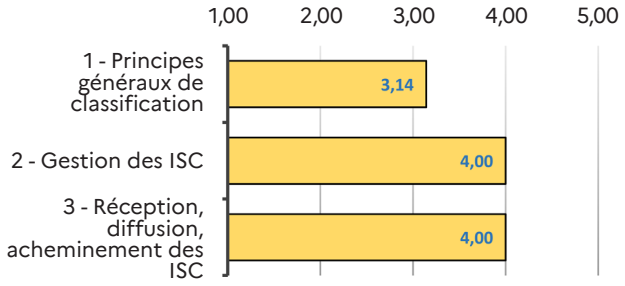
DOMAINE ORGANISATION



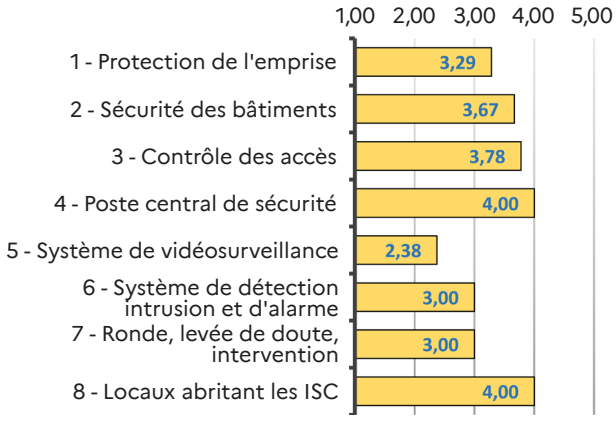
DOMAINE SÉCURITÉ DES PERSONNES



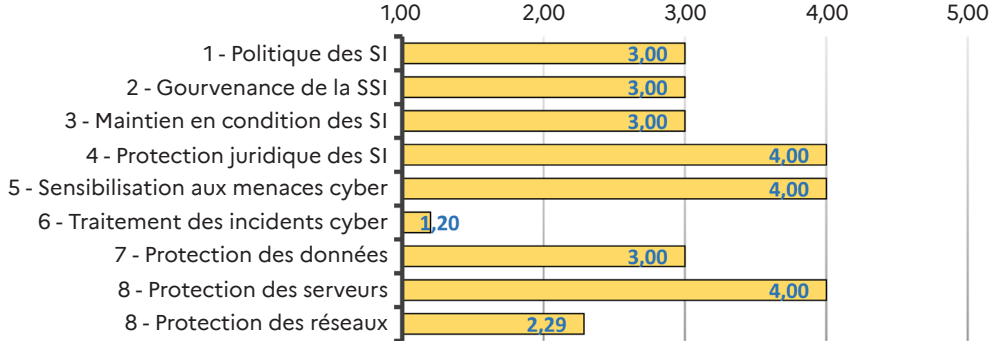
DOMAINE SÉCURITÉ DES ISC



DOMAINE SÉCURITÉ PHYSIQUE DU SITE



DOMAINE SÉCURITÉ DES SI



ÉTAPE 8 Je détermine le niveau de criticité du risque net

PONDÉRER LE NIVEAU DE CRITICITÉ DU RISQUE BRUT

Je pondère le niveau de criticité brut de chaque risque en tenant compte des mesures de sécurité existantes et des vulnérabilités que j'ai recensées dans l'étape précédente en appliquant le coefficient ci-dessous.

NIVEAU D'ÉVALUATION DES MESURES DE RÉDUCTION DES VULNÉRABILITÉS		CALCUL	
1	**MESURES ABSENTES.** Dispositif sûreté non présent ou inefficacité évidente pour réduire les vulnérabilités identifiées.	1	x Niveau de criticité brut
2	**MESURES PARTIELLES.** Dispositif sûreté incomplet ne restituant qu'une partie du service et des fonctionnalités attendus pour réduire les vulnérabilités identifiées.	0.8	
3	**MESURES DE SUBSTITUTION.** Dispositif sûreté rendant le service attendu mais sans garantie sur la durée pour réduire les vulnérabilités identifiées.	0.6	
4	**MESURES PERFORMANTES.** Dispositif sûreté garantissant une efficacité sur la durée avec optimisation des moyens pour réduire les vulnérabilités identifiées.	0.4	
5	**MESURES EXCELLENTES.** Dispositif sûreté permettant de réduire au maximum les vulnérabilités identifiées.	0.2	

DÉTERMINER LE NIVEAU DE CRITICITÉ DU RISQUE NET

Je détermine le niveau de criticité du risque net en multipliant le niveau de criticité du risque brut par le coefficient du niveau de mesure de mon dispositif sûreté.

Je peux positionner le niveau de criticité net de chaque risque sur la matrice.

MATRICE DES RISQUES

PROBABILITÉ — NOUVELLE COTATION

GRAVITÉ[2] — NOUVELLE COTATION

	G1	G2	G3	G4	G5
P5	5	20	45	80	125
P4	4	16	36	64	100
P3	3	12	27	48	75
P2	2	8	18	32	50
P1	1	4	9	16	25

Niveau de criticité NET	
Risque critique	50 à 125
Risque élevé	25 à 49
Risque moyen	12 à 24
Risque faible	1 à 11

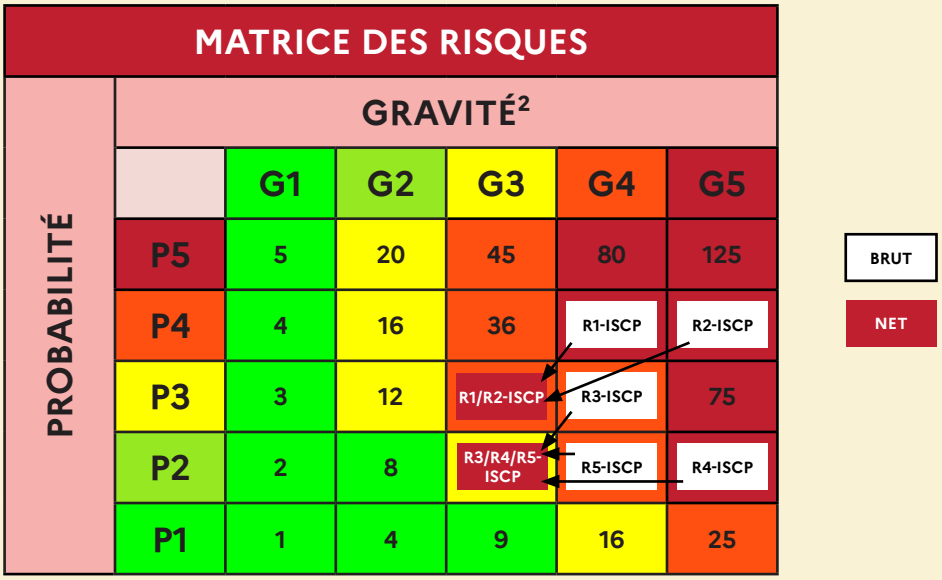
ÉTAPE 8

EXEMPLE PME FICTIVE

PONDÉRER LE NIVEAU DE CRITICITÉ DU RISQUE BRUT

DESCRIPTION DES SCÉNARIOS	P	G	CRITICITÉ BRUTE	COTATION MESURES	CRITICITÉ NETTE	RISQUE À TRAITER
Destruction volontaire de document(s) classifié(s) de la part d'un détenteur par vengeance ou manipulé par un acteur extérieur à l'organisme.	4	4	64	4	25,6	Oui
Vol de document(s) classifié(s) papier par un personnel de l'organisme.	4	5	100	3	60	Oui
Vol de document(s) classifié(s) papier suite à une intrusion (consentie ou non) par un ou des individu(s) extérieur(s) à l'organisme.	3	4	48	4	19,2	Oui
Vol de document(s) classifié(s) papier suite à une intrusion violente par un ou des individu(s) extérieur(s) à l'organisme.	2	5	50	4	20	Oui
Destruction volontaire de document(s) classifié(s) par un salarié ou un acteur extérieur à l'organisme.	2	4	32	2	25,6	Oui
... ...	...	...	...	...	...	...

DÉTERMINER LE NIVEAU DE CRITICITÉ DU RISQUE NET



Les étapes suivantes du management du risque, à savoir la mise en œuvre du plan de traitement et la surveillance et le contrôle sont identiques à la méthodologie générique développée dans la première partie de ce guide.

MAÎTRISE ET TRAITEMENT DES RISQUES

ÉTAPE 9 Je hiérarchise les risques et établis les priorités

Identifier les risques significatifs obtenus lors de l'analyse des risques me permettra de déterminer, parmi eux, les risques confirmés ou maîtrisés. Je peux alors hiérarchiser les risques significatifs et établir des priorités de traitement.

ÉTAPE 10 Je détermine des mesures de traitement

Traiter les risques significatifs a pour objectif de réduire l'exposition de mon organisation aux risques. Je dois déterminer une stratégie de traitement adaptée et établir des mesures de prévention et de protection.

SURVEILLANCE, CONTRÔLE ET RÉEXAMEN DES RISQUES

ÉTAPE 11 Je surveille, contrôle et réexamine les risques

Je dois réexaminer le plan de traitement afin de m'assurer que les mesures soient maintenues en condition opérationnelle et adaptées à l'évolution de mon environnement.

PAGE DE NOTES

GLOSSAIRE

Le glossaire se fonde sur les définitions admises par les normes ISO relatives au management des risques et adaptées à la terminologie utilisée dans le référentiel ministériel 2023 des menaces et des aléas.

ACCEPTATION DU RISQUE. Décision argumentée par le propriétaire du risque en faveur de la prise d'un risque particulier. L'acceptation du risque peut avoir lieu sans traitement du risque ou au cours du processus de traitement du risque. Les risques acceptés font l'objet d'une surveillance et d'un réexamen.

ALÉA. Manifestation d'un phénomène naturel ou anthropique. L'aléa exclut toute intention malveillante.

ANALYSE DE RISQUES. Processus mis en œuvre pour comprendre la nature des risques et pour déterminer le niveau de risques. L'analyse de risques fournit la base de l'évaluation des risques et les décisions relatives au traitement des risques. L'analyse de risques comporte six étapes :
- étude de l'environnement ;
- identification des valeurs ;
- étude des menaces et des aléas ;
- identification des risques ;
- cartographie des risques ;
- évaluation des risques.

ATTRACTIVITÉ. Mesure du degré d'attraction d'un bien, d'une personne, d'une information matérielle ou immatérielle, d'un savoir-faire, que détient un organisme, sur une échelle de cotation de 1 à 4. Le niveau 1 correspond à une cible non attractive, le niveau 4 correspond à une cible très attractive.

CIBLE. Valeur qui représente une attractivité pour un auteur de malveillance.

CONTEXTE EXTERNE. Environnement externe dans lequel l'organisme cherche à atteindre ses objectifs. Le contexte externe peut inclure :
- l'environnement culturel, social, politique, légal, réglementaire, financier, technologique, économique, naturel et concurrentiel, au niveau international, national, régional ou local ;
- les facteurs et tendances ayant un impact déterminant sur les objectifs de l'organisme ;
- les relations avec les parties prenantes externes, leurs perceptions.

CONTEXTE INTERNE. Environnement interne dans lequel l'organisme cherche à atteindre ses objectifs. Le contexte interne peut inclure :
- la gouvernance, l'organisation, les rôles et les responsabilités ;
- les politiques, les objectifs et les stratégies mises en place pour atteindre ces derniers ;
- les capacités, en termes de ressources et de connaissances (par exemple ressources humaines, capital, temps, personnels, processus, systèmes et technologies) ;
- les informations générales relatives à la volumétrie, la périmétrie et la périphérie du site, les systèmes d'information, les flux d'information et les processus de prise de décision (à la fois formels et informels) ;
- les relations avec les parties prenantes internes, ainsi que leurs perceptions et leurs valeurs ;
- la culture de l'organisme ;
- les normes, lignes directrices et modèles adoptés par l'organisme ;
- la forme et l'étendue des relations contractuelles.

CRITÈRES DE RISQUE. Termes de référence vis-à-vis desquels l'importance d'un risque est évaluée. Les critères de risque sont fondés sur les objectifs de l'organisme ainsi que sur le contexte externe et interne. Les critères de risque peuvent être issus de lois, de règlements, de normes, de politiques et d'autres exigences. Ces critères sont définis par le propriétaire du risque.

GLOSSAIRE

ÉVALUATION DU RISQUE. Processus de comparaison des résultats de l'analyse de risques avec les critères de risque et les mesures de sécurité existantes afin de déterminer si le risque et/ou son importance sont acceptables ou tolérables. L'évaluation du risque aide à la prise de décision relative au traitement du risque.

ENVIRONNEMENT. L'environnement d'une organisation correspond au contexte externe et interne dans lequel l'organisme cherche à définir et atteindre ses objectifs.

ÉVÉNEMENT. Occurrence ou changement d'un ensemble particulier de circonstances.
Un événement peut être unique ou se reproduire et peut avoir plusieurs causes.
Un événement peut consister en quelque chose qui ne se produit pas.
Un événement peut parfois être qualifié « d'incident » ou « d'accident ».
Un événement sans conséquences peut également être appelé « quasi-accident » ou « incident ».

EXPOSITION. Degré auquel un organisme est soumis à un événement.

GRAVITÉ. Mesure les effets de l'atteinte à l'organisation sur une échelle de cotation de 1 à 5. Le niveau 1 correspond à une gravité mineure, le niveau 5 correspond à une gravité critique.

IDENTIFICATION DES MENACES ET DES ALÉAS. Processus de recherche, de reconnaissance et de description des menaces et des aléas auxquels une organisation est susceptible d'être exposée.

L'identification des menaces et des aléas comprend l'identification des sources de menaces et d'aléas, des événements, de leurs causes et de leurs conséquences potentielles.

L'identification peut s'appuyer sur le catalogue ministériel des menaces et des aléas, ainsi que sur d'autres catalogues existants, conformément, le cas échéant, aux obligations légales et règlementaires.

L'identification des menaces et des aléas peut aussi faire appel à des données historiques, des analyses théoriques, des avis d'experts et autres personnes compétentes et tenir compte des besoins des parties prenantes.

MANAGEMENT DU RISQUE. Activités coordonnées dans le but de diriger et piloter un organisme vis-à-vis du risque.

MATRICE DES RISQUES. Outil permettant de classer et de visualiser des scénarios en fonction de leurs niveaux de probabilité et de gravité. Il permet de déterminer un niveau de criticité du risque.

MENACE. Manifestation signifiant une intention hostile, le projet de nuire. Elle varie en fonction de son auteur, de ses ressources, de son degré de motivation, mais aussi des capacités et vulnérabilités de l'entité menacée. Le terme de menace n'inclut pas l'exposition à un aléa.

MESURES DE SÉCURITÉ EXISTANTES. Les mesures de sécurité existantes sont toutes les mesures déjà mises en place ou prévues afin de réduire l'exposition de mon organisation à une menace ou un aléa.

MESURES DE PRÉVENTION. Dispositifs ou actions propres à diminuer la probabilité d'occurrence d'un risque, au moyen de solutions organisationnelles, techniques et humaines.

MESURES DE PROTECTION. Dispositifs ou actions propres à diminuer, réduire ou contenir les effets d'un risque après sa survenue. Les moyens de protection agissent sur la diminution des conséquences du risque, au moyen de solutions organisationnelles, techniques et humaines.

MOYEN DE MAÎTRISE. Mesure de sécurité qui modifie le niveau de criticité du risque.
Un moyen de maîtrise du risque inclut n'importe quel processus, politique, dispositif, pratique ou autre action qui modifie un risque.
Un moyen de maîtrise du risque n'aboutit pas toujours nécessairement à la modification voulue ou supposée.

GLOSSAIRE

NIVEAU DE CRITICITÉ DU RISQUE. Degré d'importance d'un risque, exprimé en termes de combinaison de la probabilité et de la gravité d'un scénario, et cartographié sur une matrice des risques.

PLAN DE TRAITEMENT. Terme générique pour désigner une procédure documentée dans laquelle une organisation décrit la façon dont elle prévoit de gérer les risques identifiés durant l'analyse de risques. Il définit les mesures de sécurité à mettre en œuvre pour rester sous le seuil d'acceptation du risque déterminé par le propriétaire du risque.

POLITIQUE DE MANAGEMENT DU RISQUE. Déclaration des intentions et des orientations générales d'un organisme en relation avec le management du risque.

PROBABILITÉ. Possibilité qu'un scénario se produise, mesurée sur une échelle de cotation de 1 à 5. Le niveau 1 correspond à une probabilité improbable, le niveau 5 correspond à une probabilité quasi-certaine.

PROCESSUS DE MANAGEMENT DU RISQUE. Application systématique de politiques, procédures et pratiques de management aux activités de communication, de concertation, d'établissement du contexte, ainsi qu'aux activités d'identification, d'analyse, d'évaluation, de traitement, de surveillance et de revue des risques.

PROPRIÉTAIRE DU RISQUE. Personne ou entité ayant la responsabilité du risque et ayant autorité pour le gérer. Il peut s'agir du responsable d'organisme ou de toute autre entité désignée par la loi ou les règlements, compte tenu du statut du site concerné et/ou de la nature de l'activité menée...

RÉEXAMEN. Activité entreprise afin de déterminer l'adaptation, l'adéquation et l'efficacité de l'objet étudié pour atteindre les objectifs établis. Le réexamen peut s'appliquer à un cadre organisationnel ou un processus relatif au management du risque ou au plan de traitement.

REFUS DU RISQUE. Décision argumentée de ne pas s'engager dans une activité, ou de s'en retirer, afin de ne pas être exposé à un risque particulier. Le refus du risque peut être fondé sur le résultat d'une évaluation du risque et/ou sur des obligations légales et réglementaires.

RISQUE. Le risque correspond à la probabilité de survenance d'un événement dommageable pouvant porter préjudice à la réalisation des objectifs d'une organisation. Il résulte de l'appréciation de deux composantes :

- la probabilité de l'événement ;
- la gravité, ou effets de l'événement.

RISQUE BRUT. Risque identifié pour l'organisme dont l'évaluation de la criticité se fait avant la prise en compte des moyens de maîtrise. Un risque brut peut être significatif ou non significatif.

RISQUE NET. Risque identifié pour l'organisme dont l'évaluation de la criticité se fait après la prise en compte des moyens de maîtrise. Un risque net peut être un risque significatif confirmé (non maîtrisé) ou un risque significatif maîtrisé.

RISQUE NON SIGNIFICATIF. Risque dont l'évaluation initiale (risque brut) est inférieure au seuil d'acceptabilité défini par le propriétaire du risque.

RISQUE RÉSIDUEL. Risque subsistant après le traitement du risque. Un risque résiduel peut inclure un risque non identifié. Un risque résiduel peut également être appelé « risque pris ».

RISQUE SIGNIFICATIF. Risque dont l'évaluation initiale (risque brut) est supérieure au seuil d'acceptabilité défini par le propriétaire du risque.

GLOSSAIRE

RISQUE SIGNIFICATIF CONFIRMÉ. Risque net dont le niveau de criticité net est supérieur au seuil d'acceptabilité défini par le propriétaire du risque. Un risque significatif confirmé correspond à un risque significatif non maîtrisé.

RISQUE SIGNIFICATIF MAÎTRISÉ. Risque net dont le niveau de criticité net est inférieur au seuil d'acceptabilité défini par le propriétaire du risque.

SCÉNARIO. Situation fictive, envisagée plausible, dans laquelle une menace ou un aléa affecte le personnel, les installations, les moyens et/ou les activités de la défense.

SEUIL D'ACCEPTATION DU RISQUE. Limite en dessous de laquelle les risques identifiés sont considérés comme maîtrisés par le propriétaire du risque, et au-dessus de laquelle ils nécessitent des moyens de maîtrise intégrés à un plan de traitement.

SURVEILLANCE. Vérification, supervision, observation critique ou détermination de l'état des menaces et des aléas afin d'identifier continûment des changements par rapport au niveau de performance exigé ou attendu. La surveillance peut s'appliquer à un cadre organisationnel de management du risque, un processus de management du risque, ou un moyen de maîtrise du risque.

TRAITEMENT DU RISQUE. Il s'agit d'un processus générique destiné à modifier un risque.

Le traitement du risque peut inclure :

- un refus du risque en décidant de ne pas démarrer ou poursuivre l'activité porteuse du risque ;
- la prise ou l'augmentation d'un risque afin de saisir une opportunité ;
- l'élimination de la source d'une menace ou d'un aléa ;
- une modification de la probabilité ;
- une modification des conséquences ;
- un partage du risque avec une ou plusieurs autres parties incluant des contrats et un financement du risque ;
- un maintien du risque fondé sur une décision argumentée.

Les traitements du risque portant sur les conséquences négatives sont parfois appelés « atténuation du risque », « élimination du risque », « prévention du risque » et « réduction du risque ». Le traitement du risque peut créer de nouveaux risques ou modifier des risques existants.

VALEUR. Une valeur est un bien, une personne, une information matérielle ou immatérielle, un savoir-faire, que détient un organisme et qui revêt un caractère précieux, voire indispensable (pour son activité, son fonctionnement, sa pérennité) et vulnérable du fait de son prix, de son attrait commercial, de son coût, de son délai de remplacement ou de son caractère unique.

VULNÉRABILITÉ. Faiblesse d'une organisation ou d'un système susceptible d'être exploitée par des menaces ou d'augmenter l'exposition aux risques.

PROBABILITÉ. Possibilité qu'un scénario se produise, mesurée sur une échelle de cotation de 1 à 5. Le niveau 1 correspond à une probabilité improbable, le niveau 5 correspond à une probabilité quasi-certaine.


DIRECTION DU RENSEIGNEMENT ET DE LA SÉCURITÉ DE LA DÉFENSE
DRSD


DIRECTION DE LA PROTECTION DES INSTALLATIONS MOYENS ET ACTIVITES DE LA DEFENSE