Modèle de rapport d'analyse de risques

Référence	Version	Date	Catégorie
MOD-CRM-005	v1.0	Janvier 2025	Commercial & Relation Client

> ***Modèle***

Ce modèle structure les rapports d'analyse de risques réalisés par Mileo Technology dans le cadre de missions de conseil en sécurité physique. La méthodologie adoptée s'inspire des normes ISO 31000 (management du risque) et de la méthode EBIOS Risk Manager de l'ANSSI, adaptée au contexte de la sécurité physique et électronique. L'objectif est de fournir au client une base rationnelle et documentée pour ses décisions d'investissement en sécurité.

---

01. Méthodologie et contexte

L'analyse de risques est conduite selon un processus en 5 étapes successives : (1) définition du contexte et des objectifs de sécurité, (2) identification et valorisation des actifs à protéger, (3) identification des menaces et évaluation de leur vraisemblance, (4) évaluation de l'impact des scénarios de risque, (5) proposition de mesures de traitement et calcul du risque résiduel. Cette approche structurée garantit l'exhaustivité de l'analyse et la traçabilité des choix.

La méthode EBIOS Risk Manager, développée par l'ANSSI pour l'analyse de risques SSI, est adaptée ici à la sécurité physique en substituant aux biens supports informatiques les éléments physiques de l'organisation (infrastructures, personnes, équipements, données physiques). Cette adaptation permet d'utiliser un référentiel reconnu et de faciliter la cohérence avec les démarches de sécurité globale (physique + numérique) que certains clients conduisent en parallèle.

---

02. Cartographie des actifs à protéger

Les actifs à protéger sont identifiés en collaboration avec le client lors d'entretiens avec les directions métier et technique. Ils sont classés en catégories : actifs physiques (équipements, matières premières, produits finis, archives physiques), actifs humains (personnes, compétences clés, informations sensibles portées par des individus), actifs informationnels (données confidentielles, propriété intellectuelle, données clients) et actifs d'image (réputation, confiance des clients, continuité de service).

Chaque actif est valorisé selon deux critères : sa valeur intrinsèque (coût de remplacement ou impact de sa perte) et son importance stratégique pour l'organisation (criticité opérationnelle). Cette valorisation est réalisée avec les représentants du client et constitue la base de priorisation des mesures de sécurité : les actifs les plus valorisés bénéficient des niveaux de protection les plus élevés.

---

03. Identification des menaces et probabilités

Les menaces sont identifiées à partir de plusieurs sources complémentaires : les retours d'expérience du secteur d'activité du client (statistiques de sinistralité, incidents déclarés dans le secteur), les informations des services de police et de gendarmerie locaux (géographie criminelle), l'analyse des menaces internes (malveillance interne, négligence) et des menaces externes (vol, intrusion, vandalisme, espionnage industriel, terrorisme selon le contexte).

La probabilité de chaque menace est évaluée sur une échelle à 4 niveaux (Rare, Peu probable, Probable, Très probable) en tenant compte de la vulnérabilité actuelle du site face à cette menace. La combinaison probabilité/impact permet de calculer le niveau de risque inhérent (avant mesures de traitement) pour chaque scénario de risque retenu.

---

04. Mesures de traitement et risque résiduel

Pour chaque scénario de risque dont le niveau inhérent est jugé inacceptable, des mesures de traitement sont proposées. Quatre options de traitement sont possibles : réduction du risque (mise en

place de mesures de sécurité réduisant la probabilité ou l'impact), transfert du risque (assurance, responsabilité contractuelle d'un tiers), acceptation du risque (décision motivée du client d'assumer le risque), ou évitement du risque (modification de l'activité ou du processus à l'origine du risque).

> **Le risque résiduel — niveau de risque subsistant après application des mesures de traitement — est calculé et présenté pour chaque scénario. Il est soumis à l'appréciation du client, qui doit formellement accepter ou refuser le risque résiduel. Les risques résiduels jugés inacceptables conduisent à la définition de mesures de traitement complémentaires ou à une révision des objectifs de sécurité. Le rapport final intègre la déclaration d'acceptation du risque résiduel signée par la direction du client.**

47 Boulevard de Courcelles, 75008 Paris — hello@mileotech.com